Benutzerhandbuch

AWS Security Hub

AWS Security Hub: Benutzerhandbuch

Table of Contents

Was ist AWS Security Hub?

AWS Security Hub bietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS und hilft Ihnen dabei, Ihre -AWSUmgebung anhand von Sicherheitsstandards und bewährten Methoden der Branche zu bewerten.

Security Hub sammelt Sicherheitsdaten über AWS-Konten, AWS-Servicesund unterstützte Drittanbieterprodukte hinweg und hilft Ihnen, Ihre Sicherheitstrends zu analysieren und Sicherheitsprobleme mit höchster Priorität zu identifizieren.

Um Sie bei der Verwaltung des Sicherheitsstatus Ihrer Organisation zu unterstützen, unterstützt Security Hub mehrere Sicherheitsstandards. Dazu gehören der AWS Foundational Security Best Practices (FSBP)-Standard, der von entwickelt wurdeAWS, sowie externe Compliance-Frameworks wie das Center for Internet Security (CIS), der Payment Card Industry Data Security Standard (PCI DSS) und das National Institute of Standards and Technology (NIST). Jeder Standard umfasst mehrere Sicherheitskontrollen, von denen jede eine bewährte Sicherheitsmethode darstellt. Security Hub führt Prüfungen anhand von Sicherheitskontrollen durch und generiert Kontrollergebnisse, die Sie bei der Bewertung Ihrer Compliance mit bewährten Sicherheitsmethoden unterstützen.

Zusätzlich zur Generierung von Kontrollergebnissen erhält Security Hub auch Ergebnisse von anderen AWS-Services– wie Amazon GuardDuty, Amazon Inspector und Amazon Macie – und unterstützten Produkten von Drittanbietern. Auf diese Weise erhalten Sie einen einzigen Glasbereich in eine Vielzahl von sicherheitsrelevanten Problemen. Sie können Security Hub-Ergebnisse auch an andere AWS-Services und unterstützte Produkte von Drittanbietern senden.

Security Hub bietet Automatisierungsfunktionen, mit denen Sie Sicherheitsprobleme beheben und beheben können. Sie können beispielsweise Automatisierungsregeln verwenden, um kritische Erkenntnisse automatisch zu aktualisieren, wenn eine Sicherheitsprüfung fehlschlägt. Sie können die Integration mit Amazon auch nutzen EventBridge , um automatische Antworten auf bestimmte Erkenntnisse auszulösen.

Themen

Vorteile von Security Hub

Hier sind einige der wichtigsten Möglichkeiten, wie Security Hub Ihnen hilft, Ihre Compliance und Ihren Sicherheitsstatus in Ihrer gesamten -AWSUmgebung zu überwachen.

Reduzierter Aufwand zur Erfassung und Priorisierung von Ergebnissen

Security Hub reduziert den Aufwand, Sicherheitserkenntnisse aus integrierten und AWS Partnerprodukten zu sammeln AWS-Services und zu priorisieren. Security Hub verarbeitet das Suchen von Daten mit dem AWS Security Finding Format (ASFF), einem Standard-Erkenntnisformat. Dadurch entfällt die Notwendigkeit, Erkenntnisse aus myriad-Quellen in mehreren Formaten zu verwalten. Security Hub korreliert auch die Erkenntnisse zwischen den Anbietern, um Ihnen zu helfen, die wichtigsten zu priorisieren.

Automatische Sicherheitsprüfungen nach bewährten Methoden und Standards

Security Hub führt automatisch kontinuierliche Konfigurations- und Sicherheitsprüfungen auf Kontoebene auf der Grundlage AWS bewährter Methoden und Branchenstandards durch. Security Hub verwendet die Ergebnisse dieser Prüfungen, um Sicherheitswerte zu berechnen, und identifiziert bestimmte Konten und Ressourcen, die Aufmerksamkeit erfordern.

Konsolidierte Ansicht der Ergebnisse über Konten und Anbieter hinweg

Security Hub konsolidiert Ihre Sicherheitserkenntnisse über Konten und Anbieterprodukte hinweg und zeigt Ergebnisse in der Security Hub-Konsole an. Sie können Ergebnisse auch über die Security Hub API, AWS CLIoder SDKs abrufen. Mit einem ganzheitlichen Überblick über Ihren aktuellen Sicherheitsstatus können Sie Trends erkennen, potenzielle Probleme identifizieren und die erforderlichen Maßnahmen ergreifen.

Möglichkeit zur Automatisierung von Aktualisierungen und Behebung von Erkenntnissen

Sie können Automatisierungsregeln erstellen, die Ergebnisse basierend auf Ihren definierten Kriterien ändern oder unterdrücken. Security Hub unterstützt auch eine Integration mit Amazon EventBridge. Um die Behebung bestimmter Erkenntnisse zu automatisieren, können Sie benutzerdefinierte Aktionen definieren, die bei der Generierung eines Ergebnisses ausgeführt werden sollen. Sie können beispielsweise benutzerdefinierte Aktionen konfigurieren, damit Ergebnisse an ein Ticketing-System oder ein automatisiertes Behebungssystem gesendet werden.

Zugriff auf Security Hub

Security Hub ist in den meisten verfügbarAWS-Regionen. Eine Liste der Regionen, in denen Security Hub derzeit verfügbar ist, finden Sie unter AWS Security Hub-Endpunkte und -Kontingente im Allgemeine AWS-Referenz. Informationen zur Verwaltung von AWS-Regionen für Ihr finden Sie unter FestlegenAWS-Konto, welche Ihr Konto verwenden kann im AWS Account Management - Referenzhandbuch. AWS-Regionen

In jeder Region können Sie auf Security Hub wie folgt zugreifen und ihn verwenden:

Security Hub-Konsole

AWS Management Console ist eine browserbasierte Schnittstelle, mit der Sie -AWSRessourcen erstellen und verwalten können. Als Teil dieser Konsole bietet die Security Hub-Konsole Zugriff auf Ihr Security Hub-Konto, Ihre Daten und Ressourcen. Sie können Security Hub-Aufgaben mithilfe der Security Hub-Konsole ausführen – Ergebnisse anzeigen, Automatisierungsregeln erstellen, eine Aggregationsregion erstellen und vieles mehr.

Security Hub API

Die Security Hub API bietet Ihnen programmatischen Zugriff auf Ihr Security Hub-Konto, Ihre Daten und Ressourcen. Mit der API können Sie HTTPS-Anforderungen direkt an Security Hub senden. Weitere Informationen zur -API finden Sie in der Referenz zur AWS Security Hub API.

AWS CLI

Mit der können Sie Befehle in der Befehlszeile Ihres Systems ausführenAWS CLI, um Security Hub-Aufgaben auszuführen. In einigen Fällen kann die Verwendung der Befehlszeile schneller und bequemer sein als die Verwendung der Konsole. Die Befehlszeile ist auch nützlich, wenn Sie Skripts erstellen möchten, die Aufgaben ausführen. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im AWS Command Line InterfaceLeitfaden.

AWS SDKs

AWS stellt SDKs bereit, die aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen bestehen, z. B. Java, Go, Python, C++ und .NET. Die -SDKs bieten praktischen, programmgesteuerten Zugriff auf Security Hub und andere AWS-Services in Ihrer bevorzugten Sprache. Sie erledigen auch Aufgaben wie kryptografisches Signieren von Anforderungen, Verwalten von Fehlern und automatisches Wiederholen von Anforderungen. Informationen zur Installation und Verwendung der -AWSSDKs finden Sie unter Tools zum Erstellen auf AWS. SDKs

> **Important**
>
> Security Hub erkennt und konsolidiert Ergebnisse, die nach der Aktivierung von Security Hub generiert werden. Es erkennt und konsolidiert Sicherheitserkenntnisse, die generiert wurden, bevor Sie Security Hub aktiviert haben, nicht rückwirkend.
> Security Hub empfängt und verarbeitet nur Ergebnisse in der Region, in der Sie Security Hub in Ihrem Konto aktiviert haben.
> Um die Sicherheitsprüfungen von CIS AWS Foundations Benchmark vollständig einzuhalten, müssen Sie Security Hub in allen unterstützten AWS Regionen aktivieren.

Zugehörige Services

Um Ihre AWS Umgebung weiter zu schützen, sollten Sie andere AWS-Services in Kombination mit Security Hub verwenden.

Eine Liste der anderen AWS-Services, die Security Hub-Ergebnisse senden oder empfangen, finden Sie unter AWS-Service Integrationen mit AWS Security Hub.

Security Hub verwendet serviceverknüpfte Regeln von AWS Config, um Sicherheitsprüfungen für die meisten Kontrollen durchzuführen. Sie müssen Ressourcen in AWS Config für Security Hub aktivieren AWS Config und aufzeichnen, um die meisten Kontrollergebnisse zu generieren. Weitere Informationen finden Sie unter Konfiguration AWS Config.

Kostenlose Testversion und Preise für Security Hub

Wenn Sie Security Hub AWS-Konto zum ersten Mal in einem aktivieren, wird dieses Konto automatisch in einer 30-tägigen kostenlosen Security Hub-Testversion registriert.

Wenn Sie Security Hub während der kostenlosen Testversion verwenden, wird Ihnen die Nutzung anderer Services, mit denen Security Hub interagiert, wie z. B. AWS Config Elemente, in Rechnung gestellt. AWS Config Regeln, die nur durch Security Hub-Sicherheitsstandards aktiviert werden, werden Ihnen nicht in Rechnung gestellt.

Die Nutzung von Security Hub wird Ihnen erst in Rechnung gestellt, wenn Ihre kostenlose Testversion endet.

> **Note**
>
> Die kostenlose Testversion von Security Hub wird in der Region China (Peking) nicht unterstützt.

Anzeigen von Nutzungsdetails und geschätzten Kosten

Security Hub stellt Nutzungsinformationen bereit, einschließlich der geschätzten 30-Tage-Kosten für die Verwendung von Security Hub. Die Nutzungsdetails beinhalten die verbleibende Zeit in der kostenlosen Testversion. Die Nutzungsinformationen können Ihnen helfen, zu verstehen, wie hoch Ihre Security Hub-Kosten nach Ablauf der kostenlosen Testversion sein könnten. Die Nutzungsinformationen sind auch nach Ablauf der kostenlosen Testversion verfügbar.

So zeigen Sie Nutzungsinformationen an (Konsole)

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Verwendung aus.

Die geschätzten monatlichen Kosten basieren auf der Security Hub-Nutzung Ihres Kontos für Erkenntnisse und Sicherheitsprüfungen, die über einen Zeitraum von 30 Tagen prognostiziert werden.

Die Nutzungsinformationen und die geschätzten Kosten beziehen sich nur auf das aktuelle Konto und die aktuelle Region. In einer Aggregationsregion enthalten die Nutzungsinformationen und die geschätzten Kosten keine verknüpften Regionen. Weitere Informationen zu verknüpften Regionen finden Sie unter the section called “So funktioniert die regionsübergreifende Aggregation”.

Preisdetails

Weitere Informationen darüber, wie Security Hub Gebühren für aufgenommene Erkenntnisse und Sicherheitsprüfungen berechnet, finden Sie unter Security Hub – Preise.

Security Hub Hub-Konzepte

In diesem Thema werden die wichtigsten Konzepte und Begriffe in AWS Security Hub beschrieben, um Ihnen den Einstieg in den Service zu erleichtern.

Account

Ein Standardkonto von Amazon Web Services (AWS), das Ihre AWS Ressourcen enthält. Sie können sich AWS mit Ihrem Konto anmelden und Security Hub aktivieren.

Ein Konto kann andere Konten zur Aktivierung von Security Hub einladen und mit diesem Konto in Security Hub verknüpft werden. Das Annehmen einer Mitgliedschaftseinladung ist optional. Wenn die Einladungen akzeptiert werden, wird das Konto zu einem Administratorkonto und die hinzugefügten Konten sind Mitgliedskonten. Administratorkonten können Ergebnisse in ihren Mitgliedskonten einsehen.

Wenn Sie registriert sind AWS Organizations, weist Ihre Organisation ein Security Hub-Administratorkonto für die Organisation zu. Das Security Hub-Administratorkonto kann andere Unternehmenskonten als Mitgliedskonten aktivieren.

Ein Konto kann nicht gleichzeitig Administratorkonto und Mitgliedskonto sein. Ein Konto kann nur ein Administratorkonto haben.

Weitere Informationen finden Sie unter Verwaltung von Administrator- und Mitgliedskonten.

Administratorkonto

Ein Konto in Security Hub, dem Zugriff gewährt wird, um Ergebnisse für verknüpfte Mitgliedskonten einzusehen.

Ein Konto wird auf eine der folgenden Arten zu einem Administratorkonto:

- Das Konto lädt andere Konten ein, ihm in Security Hub zugeordnet zu werden. Wenn diese Konten die Einladung annehmen, werden sie zu Mitgliedskonten und das einladende Konto wird zu ihrem Administratorkonto.
- Das Konto wird von einem Organisationsverwaltungskonto als Security Hub-Administratorkonto festgelegt. Das Security Hub-Administratorkonto kann jedes Unternehmenskonto als Mitgliedskonto aktivieren und auch andere Konten zu Mitgliedskonten einladen.

Ein Konto kann nur ein Administratorkonto haben. Ein Konto kann nicht gleichzeitig ein Administratorkonto und ein Mitgliedskonto sein.

Aggregationsregion

Wenn Sie eine Aggregationsregion festlegen, können Sie Sicherheitsergebnisse aus mehreren Bereichen AWS-Regionen in einem einzigen Fenster anzeigen.

Die Aggregationsregion ist die Region, von der aus Sie Ergebnisse anzeigen und verwalten. Die Ergebnisse werden aus verknüpften Regionen zur Aggregationsregion aggregiert. Aktualisierungen der Ergebnisse werden in allen Regionen repliziert.

In der Aggregationsregion enthalten die Seiten Sicherheitsstandards, Einblicke und Ergebnisse Daten aus allen verknüpften Regionen.

Siehe Regionsübergreifende Aggregation.

Archiviertes Ergebnis

Ein Fund, bei dem `RecordState` auf `ARCHIVED` festgelegt ist. Die Archivierung eines Ergebnisses weist darauf hin, dass der Ergebnisanbieter der Ansicht ist, dass das Ergebnis nicht mehr relevant ist. Der Datensatzstatus ist unabhängig vom Workflow-Status, der den Status einer Untersuchung eines Ergebnisses verfolgt.

Finding-Provider können den `BatchImportFindings`Betrieb der Security Hub Hub-API nutzen, um von ihnen erstellte Ergebnisse zu archivieren. Security Hub archiviert automatisch Ergebnisse für Kontrollen, wenn die Steuerung deaktiviert oder die zugehörige Ressource gelöscht wird, basierend auf einem der folgenden Kriterien.

- Das Ergebnis wird nicht innerhalb von drei bis fünf Tagen aktualisiert (beachten Sie, dass dies nach bestem Wissen erfolgt und nicht garantiert wird).
- Die zugehörige AWS Config Bewertung wird zurückgegeben`NOT_APPLICABLE`.

Standardmäßig werden archivierte Ergebnisse aus den Ergebnislisten in der Security Hub Hub-Konsole ausgeschlossen. Sie können den Filter so aktualisieren, dass archivierte Ergebnisse einbezogen werden.

Der `GetFindings`Betrieb der Security Hub Hub-API gibt sowohl aktive als auch archivierte Ergebnisse zurück. Sie können einen Filter für den Datensatzstatus einschließen.

```
"RecordState": [
    {
        "Comparison": "EQUALS",
        "Value": "ARCHIVED"
    }
```

```
],
```

AWS Format für Sicherheitsbefunde (ASFF)

Ein standardisiertes Format für den Inhalt von Ergebnissen, die Security Hub aggregiert oder generiert. Mit dem AWS Security Finding Format können Sie Security Hub verwenden, um Ergebnisse anzuzeigen und zu analysieren, die von AWS Sicherheitsdiensten, Drittanbieterlösungen oder Security Hub selbst bei der Durchführung von Sicherheitsüberprüfungen generiert wurden. Weitere Informationen finden Sie unter AWS Format für Sicherheitssuche (ASFF).

Kontrolle

Eine Schutz- oder Gegenmaßnahme, die für ein Informationssystem oder eine Organisation vorgeschrieben ist, um die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationen zu schützen und eine Reihe definierter Sicherheitsanforderungen zu erfüllen. Ein Sicherheitsstandard ist mit einer Sammlung von Kontrollen verknüpft.

Der Begriff Sicherheitskontrolle bezieht sich auf Kontrollen, die standardübergreifend über eine einzige Kontroll-ID und einen einzigen Titel verfügen. Der Begriff Standardkontrolle bezieht sich auf Steuerelemente mit standardspezifischen Kontroll-IDs und Titeln. Derzeit unterstützt Security Hub nur Standardsteuerungen in den Regionen AWS GovCloud (US) Region und China. Sicherheitskontrollen werden in allen anderen Regionen unterstützt.

Benutzerdefinierte Aktion

Ein Security Hub Hub-Mechanismus zum Senden ausgewählter Ergebnisse an EventBridge. Eine benutzerdefinierte Aktion wird in Security Hub erstellt. Sie wird dann mit einer EventBridge Regel verknüpft. Die Regel definiert eine bestimmte Aktion, die ausgeführt werden soll, wenn Funde empfangen werden, die der benutzerdefinierten Aktions-ID zugeordnet sind. Benutzerdefinierte Aktionen können beispielsweise verwendet werden, um einen bestimmten Fund oder einen kleinen Satz von Funden an einen Antwort- oder Korrektur-Workflow zu senden. Weitere Informationen finden Sie unter the section called “Eine benutzerdefinierte Aktion erstellen (Konsole)”.

Delegiertes Administratorkonto (Organizations)

In Organizations kann das delegierte Administratorkonto für einen Dienst die Nutzung eines Dienstes für die Organisation verwalten.

In Security Hub ist das Security Hub-Administratorkonto auch das delegierte Administratorkonto für Security Hub. Wenn das Organisationsverwaltungskonto zum ersten Mal ein Security Hub-

Administratorkonto festlegt, ruft Security Hub Organizations auf, dieses Konto zum delegierten Administratorkonto zu machen.

Das Organisationsverwaltungskonto muss dann das delegierte Administratorkonto als Security Hub-Administratorkonto in allen Regionen auswählen.

Erkenntnis

Der beobachtbare Datensatz einer Sicherheitsprüfung oder sicherheitsrelevanten Erkennung. Security Hub generiert einen Befund, nachdem eine Sicherheitsüberprüfung einer Kontrolle abgeschlossen wurde. Diese Ergebnisse werden als Kontrollbefunde bezeichnet. Die Ergebnisse können auch aus Produktintegrationen von Drittanbietern stammen.

Weitere Informationen zu den Ergebnissen in Security Hub finden Sie unterFunde.

> **Note**
>
> Erkenntnisse werden 90 Tage nach der letzten Aktualisierung gelöscht – oder 90 Tage nach ihrer Erstellung, wenn es keine Aktualisierungen gibt. Um Ergebnisse länger als 90 Tage zu speichern, können Sie eine Regel konfigurieren, EventBridge die Ergebnisse an Ihren Amazon S3-Bucket weiterleitet.

Regionsübergreifende Aggregation

Die Zusammenfassung von Ergebnissen, Erkenntnissen, Compliance-Status und Sicherheitsbewertungen aus verknüpften Regionen zu einer Aggregationsregion. Anschließend können Sie alle Ihre Daten aus der Aggregationsregion anzeigen und die Ergebnisse und Erkenntnisse aus der Aggregationsregion aktualisieren.

Siehe Regionsübergreifende Aggregation.

Erfassung ermitteln

Der Import von Ergebnissen aus anderen AWS Diensten und von Drittanbietern in Security Hub.

Zu den festgestellten Ingestion-Ereignissen gehören sowohl neue Erkenntnisse als auch Aktualisierungen vorhandener Ergebnisse.

Insight

Eine Sammlung zusammenhängender Funde, die durch eine Aggregationsanweisung und optionale Filter definiert wird. Ein Insight identifiziert einen Sicherheitsbereich, der Aufmerksamkeit

und Intervention erfordert. Security Hub bietet mehrere verwaltete (Standard-) Einblicke, die Sie nicht ändern können. Sie können auch benutzerdefinierte Security Hub Hub-Einblicke erstellen, um Sicherheitsprobleme zu verfolgen, die für Ihre AWS Umgebung und Nutzung spezifisch sind. Weitere Informationen finden Sie unter Insights.

Verknüpfte Region

Wenn Sie die regionsübergreifende Aggregation aktivieren, ist eine verknüpfte Region eine Region, die Ergebnisse, Erkenntnisse, den Status der Kontrollkonformität und Sicherheitsbewertungen in der Aggregationsregion zusammenfasst.

In einer verknüpften Region enthalten die Seiten „Ergebnisse“ und „Einblicke“ nur Ergebnisse aus dieser Region.

Siehe Regionsübergreifende Aggregation.

Mitgliedskonto

Ein Konto, das einem Administratorkonto die Erlaubnis erteilt hat, die Ergebnisse einzusehen und entsprechende Maßnahmen zu ergreifen.

Ein Konto wird auf eine der folgenden Arten zu einem Mitgliedskonto:

- Das Konto akzeptiert eine Einladung von einem anderen Konto.
- Für ein Organisationskonto aktiviert das Security Hub-Administratorkonto das Konto als Mitgliedskonto.

Zugehörige Anforderungen

Eine Reihe von Branchen- oder regulatorischen Anforderungen, die einem Steuerelement zugeordnet sind.

Regel

Eine Reihe von automatisierten Kriterien, die verwendet werden, um zu beurteilen, ob ein Steuerelement eingehalten wird. Wenn eine Regel ausgewertet wird, kann sie erfolgreich sein oder fehlschlagen. Wenn die Auswertung nicht feststellen kann, ob die Regel erfolgreich ist oder fehlschlägt, befindet sich die Regel in einem Warnzustand. Wenn die Regel nicht ausgewertet werden kann, befindet sie sich in einem nicht verfügbaren Zustand.

Sicherheitsüberprüfung

Eine spezifische point-in-time Auswertung einer Regel anhand einer einzelnen Ressource, die zu einem Status „Bestanden“, „Fehlgeschlagen“, „Warnung“ oder „Nicht verfügbar“ führt. Das Ausführen einer Sicherheitsprüfung führt zu einem Ergebnis.

Security Hub-Administratorkonto

Ein Organisationskonto, das die Security Hub Hub-Mitgliedschaft für eine Organisation verwaltet.

Das Organisationsverwaltungskonto bestimmt das Security Hub-Administratorkonto in jeder Region. Das Organisationsverwaltungskonto muss in allen Regionen dasselbe Security Hub-Administratorkonto wählen.

Das Security Hub-Administratorkonto ist auch das delegierte Administratorkonto für Security Hub in Organizations.

Das Security Hub-Administratorkonto kann jedes Unternehmenskonto als Mitgliedskonto aktivieren. Das Security Hub-Administratorkonto kann auch andere Konten als Mitgliedskonten einladen.

Sicherheitsstandard

Eine veröffentlichte Erklärung zu einem Thema, in der die Eigenschaften (in der Regel messbar und in Form von Kontrollen) definiert sind, die gegeben sein oder erreicht werden müssen, um Compliance sicherzustellen. Sicherheitsstandards können auf regulatorischen Rahmenbedingungen, bewährten Methoden oder internen Unternehmensrichtlinien basieren. Ein Steuerelement kann mit einem oder mehreren unterstützten Standards in Security Hub verknüpft sein. Weitere Informationen zu den Sicherheitsstandards in Security Hub finden Sie unterStandards und Kontrollen.

Schweregrad

Der Schweregrad, der einem Security Hub-Steuerelement zugewiesen wurde, zeigt die Wichtigkeit der Kontrolle an. Der Schweregrad einer Kontrolle kann „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ oder „Informativ“ sein. Der den Kontrollbefunden zugewiesene Schweregrad entspricht dem Schweregrad der Kontrolle selbst. Informationen darüber, wie Security Hub einer Kontrolle den Schweregrad zuweist, finden Sie unterDen Kontrollergebnissen den Schweregrad zuweisen.

Workflow-Status

Der Status einer Untersuchung zu einem Befund. Nachverfolgt mit dem Attribut `Workflow.Status`.

Der Workflow-Status ist zunächst `NEW`. Wenn Sie den Ressourcenbesitzer benachrichtigt haben, Maßnahmen für das Ergebnis zu ergreifen, können Sie den Workflow-Status auf `NOTIFIED` festlegen. Wenn die Suche kein Problem darstellt und keine Aktion erfordert, legen Sie den

Workflow-Status auf `SUPPRESSED` fest. Nachdem Sie eine Suche überprüft und korrigiert haben, legen Sie den Workflow-Status auf `RESOLVED` fest.

Standardmäßig enthalten die meisten Suchlisten nur Ergebnisse mit dem Workflow-Status `NEW` oder `NOTIFIED`. Die Suche nach Listen für Steuerelemente umfasst auch `RESOLVED`-Ergebnisse.

Für die Operation `GetFindings` können Sie einen Filter für den Workflow-Status einschließen.

```
"WorkflowStatus": [
    {
        "Comparison": "EQUALS",
        "Value": "RESOLVED"
    }
],
```

Die Security Hub Hub-Konsole bietet eine Option, um den Workflow-Status für Ergebnisse festzulegen. Kunden (oder SIEM-, Ticketing-, Vorfallmanagement- oder SOAR-Tools, die im Auftrag eines Kunden Ergebnisse von Ergebnisanbietern aktualisieren) können mithilfe von `BatchUpdateFindings` auch den Workflow-Status aktualisieren.

Empfehlungen vor der Aktivierung von Security Hub

Die folgenden Empfehlungen können Ihnen den Einstieg in die Verwendung erleichtern AWS Security Hub.

Integration mit AWS Organizations

AWS Organizations ist ein globaler Kontoverwaltungsdienst, der es AWS Administratoren ermöglicht, mehrere Organisationseinheiten (OUs) zu konsolidieren AWS-Konten und zentral zu verwalten. Er bietet Funktionen zur Kontoverwaltung und konsolidierten Fakturierung, die auf die Erfüllung von Haushalts-, Sicherheits- und Compliance-Anforderungen zugeschnitten sind. Es wird ohne zusätzliche Kosten angeboten und lässt sich in mehrere integrieren AWS-Services, darunter Security Hub GuardDuty, Amazon und Amazon Macie.

Um die Verwaltung von Konten zu automatisieren und zu optimieren, empfehlen wir dringend, Security Hub und AWS Organizations zu integrieren. Sie können eine Integration mit Organizations durchführen, wenn Sie mehrere haben AWS-Konto , die Security Hub verwenden.

Anweisungen zur Aktivierung der Integration finden Sie unterIntegrieren von Security Hub mit AWS Organizations.

Verwenden der zentralen Konfiguration

Wenn Sie Security Hub and Organizations integrieren, haben Sie die Möglichkeit, eine Funktion namens zentrale Konfiguration zu verwenden, um Security Hub für Ihr Unternehmen einzurichten und zu verwalten. Wir empfehlen dringend, die zentrale Konfiguration zu verwenden, da der Administrator so den Sicherheitsschutz für das Unternehmen anpassen kann. Gegebenenfalls kann der delegierte Administrator einem Mitgliedskonto gestatten, seine eigenen Sicherheitseinstellungen zu konfigurieren.

Die zentrale Konfiguration ermöglicht es dem delegierten Administrator, Security Hub für Konten, Organisationseinheiten und Regionen zu konfigurieren. Der delegierte Administrator konfiguriert Security Hub, indem er Konfigurationsrichtlinien erstellt. In einer Konfigurationsrichtlinie können Sie die folgenden Einstellungen angeben:

- Ob Security Hub aktiviert oder deaktiviert ist
- Welche Sicherheitsstandards sind aktiviert und deaktiviert

- Welche Sicherheitskontrollen sind aktiviert und deaktiviert
- Ob Parameter für ausgewählte Steuerelemente angepasst werden sollen

Als delegierter Administrator können Sie eine einzige Konfigurationsrichtlinie für Ihre gesamte Organisation oder verschiedene Konfigurationsrichtlinien für Ihre verschiedenen Konten und Organisationseinheiten erstellen. Beispielsweise können Testkonten und Produktionskonten unterschiedliche Konfigurationsrichtlinien verwenden.

Mitgliedskonten und Organisationseinheiten, die eine Konfigurationsrichtlinie verwenden, werden zentral verwaltet und können nur vom delegierten Administrator konfiguriert werden. Der delegierte Administrator kann bestimmte Mitgliedskonten und Organisationseinheiten als selbstverwaltet kennzeichnen, sodass das Mitglied seine eigenen Einstellungen für jede Region konfigurieren kann.

Weitere Informationen zur zentralen Konfiguration finden Sie unter. So funktioniert die zentrale Konfiguration

Konfiguration AWS Config

AWS Security Hub verwendet dienstbezogene AWS Config Regeln, um Sicherheitsüberprüfungen für die meisten Kontrollen durchzuführen.

Um diese Kontrollen zu unterstützen, AWS Config muss sie für alle Konten — sowohl für das Administratorkonto als auch für die Mitgliedskonten — in allen AWS-Region Konten aktiviert sein, in denen Security Hub aktiviert ist. Darüber hinaus AWS Config muss für jeden aktivierten Standard so konfiguriert werden, dass er Ressourcen aufzeichnet, die für aktivierte Kontrollen erforderlich sind.

Wir empfehlen, die Ressourcenaufzeichnung zu aktivieren, AWS Config bevor Sie die Security Hub Hub-Standards aktivieren. Wenn Security Hub versucht, Sicherheitsüberprüfungen durchzuführen, obwohl die Ressourcenaufzeichnung ausgeschaltet ist, geben die Prüfungen Fehler zurück.

Security Hub verwaltet nicht AWS Config für Sie. Wenn Sie die Aktivierung bereits AWS Config aktiviert haben, können Sie die Einstellungen über die AWS Config Konsole oder APIs konfigurieren.

Wenn Sie einen Standard aktivieren, ihn aber nicht aktiviert haben AWS Config, versucht Security Hub, die AWS Config Regeln gemäß dem folgenden Zeitplan zu erstellen:

- An dem Tag, an dem Sie den Standard aktivieren
- Am Tag, nachdem Sie den Standard aktiviert haben
- 3 Tage, nachdem Sie den Standard aktiviert haben

- 7 Tage nach der Aktivierung des Standards (und danach kontinuierlich alle 7 Tage)

Wenn Sie die zentrale Konfiguration verwenden, versucht Security Hub auch, die AWS Config Regeln zu erstellen, wenn Sie eine Konfigurationsrichtlinie erneut anwenden, die einen oder mehrere Standards aktiviert.

Aktivieren AWS Config

Wenn Sie es noch nicht aktiviert AWS Config haben, können Sie es auf eine der folgenden Arten aktivieren:

- Konsole oder AWS CLI — Sie können die Aktivierung manuell AWS Config über die AWS Config Konsole oder durchführen AWS CLI. Weitere Informationen finden Sie unter Erste Schritte mit AWS Config im AWS Config Entwicklerhandbuch.
- AWS CloudFormation Vorlage — Wenn Sie die Aktivierung AWS Config für eine große Anzahl von Konten durchführen möchten, können Sie die Aktivierung AWS Config mit der CloudFormation Vorlage Enable durchführen AWS Config. Informationen zum Zugriff auf diese Vorlage finden Sie in den AWS CloudFormation StackSets Beispielvorlagen im AWS CloudFormation Benutzerhandbuch.
- Github-Skript — Security Hub bietet ein GitHub Skript, das Security Hub für mehrere Konten in verschiedenen Regionen aktiviert. Dieses Skript ist nützlich, wenn Sie keine Integration mit Organizations haben oder wenn Sie Konten haben, die nicht Teil Ihrer Organisation sind. Wenn Sie dieses Skript verwenden, um Security Hub zu aktivieren, wird es auch automatisch AWS Config für diese Konten aktiviert.

Weitere Informationen zur Aktivierung AWS Config , um Sie bei der Durchführung von Security Hub-Sicherheitsprüfungen zu unterstützen, finden Sie unter Optimieren AWS Config für, AWS Security Hub um Ihren Cloud-Sicherheitsstatus effektiv zu verwalten.

Aktivieren Sie die Ressourcenaufzeichnung in AWS Config

Wenn Sie die Ressourcenaufzeichnung AWS Config mit den Standardeinstellungen aktivieren, werden alle unterstützten Typen von regionalen Ressourcen aufgezeichnet, die in der AWS Config Umgebung erkannt werden, AWS-Region in der sie ausgeführt wird. Sie können auch so konfigurieren AWS Config , dass unterstützte Typen globaler Ressourcen aufgezeichnet werden. Sie müssen globale Ressourcen nur in einer einzigen Region aufzeichnen (wir empfehlen, dass dies Ihre Heimatregion ist, wenn Sie die zentrale Konfiguration verwenden).

Wenn Sie CloudFormation StackSets die Option aktivieren verwenden AWS Config, empfehlen wir, zwei verschiedene auszuführen StackSets. Führen Sie einen aus, StackSet um alle Ressourcen, einschließlich globaler Ressourcen, in einer einzigen Region aufzuzeichnen. Führen Sie einen zweiten StackSet Vorgang aus, um alle Ressourcen außer globalen Ressourcen in anderen Regionen aufzuzeichnen.

Sie können auch Quick Setup, eine Funktion von AWS Systems Manager, verwenden, um die Ressourcenaufzeichnung in AWS Config Ihren Konten und Regionen schnell zu konfigurieren. Während des Quick Setup-Vorgangs können Sie auswählen, in welcher Region Sie globale Ressourcen aufzeichnen möchten. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter AWS Config Configuration Recorder.

Die Sicherheitskontrolle Config.1 führt in Regionen, in denen globale Ressourcen nicht erfasst sind, zu fehlgeschlagenen Ergebnissen. Dies ist zu erwarten, und Sie können eine Automatisierungsregel verwenden, um diese Ergebnisse zu unterdrücken.

Wenn Sie das Skript für mehrere Konten verwenden, um Security Hub zu aktivieren, aktiviert es automatisch die Ressourcenaufzeichnung für alle Ressourcen, einschließlich globaler Ressourcen, in allen Regionen. Anschließend können Sie die Konfiguration so aktualisieren, dass globale Ressourcen nur in einer einzigen Region aufgezeichnet werden. Weitere Informationen finden Sie im AWS Config Entwicklerhandbuch unter Auswahl der AWS Config Ressourceneinträge.

Damit Security Hub die Ergebnisse von Kontrollen, die auf AWS Config Regeln basieren, korrekt melden kann, müssen Sie die Aufzeichnung für die entsprechenden Ressourcen aktivieren. Eine Liste der Kontrollen und der zugehörigen AWS Config Ressourcen finden Sie unterAWS Config Ressourcen, die zur Generierung der Kontrollergebnisse erforderlich sind.AWS Config ermöglicht es Ihnen, zwischen kontinuierlicher Aufzeichnung und täglicher Aufzeichnung von Änderungen des Ressourcenstatus zu wählen. Wenn Sie die tägliche Aufzeichnung wählen AWS Config , werden die Ressourcenkonfigurationsdaten am Ende jedes 24-Stunden-Zeitraums bereitgestellt, wenn sich der Ressourcenstatus ändert. Wenn es keine Änderungen gibt, werden keine Daten geliefert. Dies kann die Generierung von Security Hub Hub-Ergebnissen für durch Änderungen ausgelöste Kontrollen verzögern, bis ein Zeitraum von 24 Stunden abgeschlossen ist.

> **Note**
>
> Um nach Sicherheitsprüfungen neue Ergebnisse zu generieren und veraltete Ergebnisse zu vermeiden, benötigen Sie ausreichende Berechtigungen für die IAM-Rolle, die dem Konfigurationsrekorder zugeordnet ist, um die zugrunde liegenden Ressourcen auszuwerten.

Kostenüberlegungen

Einzelheiten zu den Kosten im Zusammenhang mit der Erfassung von Ressourcen finden Sie unter AWS Security Hub Preise und AWS Config Preisgestaltung.

Security Hub kann sich durch die Aktualisierung des AWS Config Konfigurationselements auf Ihre Kosten für den `AWS::Config::ResourceCompliance` Konfigurationsrekorder auswirken. Updates können jedes Mal erfolgen, wenn ein mit einer AWS Config Regel verknüpftes Security Hub-Steuerelement den Konformitätsstatus ändert, aktiviert oder deaktiviert wird oder Parameter-Updates enthält. Wenn Sie den AWS Config Konfigurationsrekorder nur für Security Hub verwenden und dieses Konfigurationselement nicht für andere Zwecke verwenden, empfehlen wir, die Aufzeichnung dafür in der AWS Config Konsole oder zu deaktivieren AWS CLI. Dies kann Ihre AWS Config Kosten senken. Sie müssen keine Aufzeichnungen machen, damit `AWS::Config::ResourceCompliance` die Sicherheitschecks in Security Hub funktionieren.

Security Hub aktivieren

Es gibt zwei Möglichkeiten, AWS Security Hub zu aktivieren: durch Integration mit AWS Organizations oder manuell.

Wir empfehlen dringend die Integration mit Organizations für Umgebungen mit mehreren Konten und mehreren Regionen. Wenn Sie ein eigenständiges Konto haben, müssen Sie Security Hub manuell einrichten.

Überprüfung der erforderlichen Berechtigungen

Nachdem Sie sich für Amazon Web Services (AWS) angemeldet haben, müssen Sie Security Hub aktivieren, um seine Funktionen und Funktionen nutzen zu können. Um Security Hub zu aktivieren, müssen Sie zunächst Berechtigungen einrichten, die Ihnen den Zugriff auf die Security Hub Hub-Konsole und API-Operationen ermöglichen. Sie oder Ihr AWS Administrator können dies tun, indem Sie AWS Identity and Access Management (IAM) verwenden, um die AWS verwaltete Richtlinie, die aufgerufen wird`AWSSecurityHubFullAccess`, an Ihre IAM-Identität anzuhängen.

Um Security Hub über die Organizationsintegration zu aktivieren und zu verwalten, sollten Sie auch die angegebene AWS verwaltete Richtlinie anhängen`AWSSecurityHubOrganizationsAccess`.

Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für AWS Security Hub.

Aktivierung von Security Hub mit Unternehmensintegration

Um Security Hub mit zu verwendenAWS Organizations, legt das AWS Organizations Verwaltungskonto für die Organisation ein Konto als delegiertes Security Hub-Administratorkonto für die Organisation fest. Security Hub wird automatisch im delegierten Administratorkonto in der aktuellen Region aktiviert.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zur Benennung des delegierten Administrators.

Security Hub console

So bestimmen Sie beim Onboarding den delegierten Security Hub-Administrator

1. Öffnen Sie die AWS Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/.

2. Wählen Sie Gehe zu Security Hub. Sie werden aufgefordert, sich beim Verwaltungskonto der Organizations anzumelden.
3. Geben Sie auf der Seite Delegierten Administrator benennen im Abschnitt Delegiertes Administratorkonto das delegierte Administratorkonto an. Wir empfehlen, denselben delegierten Administrator zu wählen, den Sie für andere AWS Sicherheits- und Compliance-Dienste eingerichtet haben.
4. Wählen Sie Als delegierten Administrator festlegen aus.

Security Hub API

Rufen Sie die `EnableOrganizationAdminAccount`API über das Verwaltungskonto der Organizations auf. Geben Sie die AWS-Konto ID des delegierten Security Hub-Administratorkontos an.

AWS CLI

Führen Sie den `enable-organization-admin-account`Befehl über das Verwaltungskonto der Organizations. Geben Sie die AWS-Konto ID des delegierten Security Hub-Administratorkontos an.

Beispielbefehl:

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

Weitere Informationen zur Integration mit Organizations finden Sie unterIntegrieren von Security Hub mit AWS Organizations.

Nachdem Sie den delegierten Administrator benannt haben, empfehlen wir, mit der Einrichtung von Security Hub mit zentraler Konfiguration fortzufahren. Die Konsole fordert Sie dazu auf. Durch die zentrale Konfiguration können Sie den Prozess der Aktivierung und Konfiguration von Security Hub für Ihr Unternehmen vereinfachen und sicherstellen, dass Ihr Unternehmen über eine angemessene Sicherheitsabdeckung verfügt.

Durch die zentrale Konfiguration kann der delegierte Administrator Security Hub für mehrere Unternehmenskonten und Regionen anpassen, anstatt es von Region zu Region zu konfigurieren. Sie können eine Konfigurationsrichtlinie für Ihr gesamtes Unternehmen oder unterschiedliche Konfigurationsrichtlinien für verschiedene Konten und Organisationseinheiten erstellen. Die

Richtlinien geben an, ob Security Hub in den zugehörigen Konten aktiviert oder deaktiviert ist und welche Sicherheitsstandards und Kontrollen aktiviert sind.

Der delegierte Administrator kann Konten als zentral verwaltet oder selbstverwaltet kennzeichnen. Zentral verwaltete Konten können nur vom delegierten Administrator konfiguriert werden. Selbstverwaltete Konten können ihre eigenen Einstellungen angeben.

Wenn Sie die zentrale Konfiguration nicht verwenden, kann der delegierte Administrator Security Hub nur eingeschränkt konfigurieren. Weitere Informationen finden Sie unter Konten verwalten mit AWS Organizations.

Manuelles Aktivieren von Security Hub

Sie müssen Security Hub manuell aktivieren, wenn Sie ein eigenständiges Konto haben oder wenn Sie es nicht integrierenAWS Organizations. Eigenständige Konten können nicht integriert werden AWS Organizations und müssen manuell aktiviert werden.

Wenn Sie Security Hub manuell aktivieren, legen Sie ein Security Hub-Administratorkonto fest und laden andere Konten ein, Mitgliedskonten zu werden. Die Beziehung zwischen Administrator und Mitglied wird hergestellt, wenn ein potenzielles Mitgliedskonto die Einladung annimmt.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um Security Hub zu aktivieren. Wenn Sie Security Hub von der Konsole aus aktivieren, haben Sie auch die Möglichkeit, die unterstützten Sicherheitsstandards zu aktivieren.

Security Hub console

1. Öffnen Sie die AWS Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wenn Sie die Security Hub-Konsole zum ersten Mal öffnen, wählen Sie Gehe zu Security Hub.
3. Auf der Willkommensseite werden im Abschnitt Sicherheitsstandards die Sicherheitsstandards aufgeführt, die Security Hub unterstützt.

   Aktivieren Sie das Kontrollkästchen für einen Standard, um ihn zu aktivieren, und deaktivieren Sie das Kontrollkästchen, um ihn zu deaktivieren.

Sie können einen Standard oder seine einzelnen Steuerelemente jederzeit aktivieren oder deaktivieren. Informationen zur Verwaltung von Sicherheitsstandards und -kontrollen finden Sie unter Sicherheitskontrollen und -standards in AWS Security Hub.

4. Wählen Sie Enable Security Hub (Security Hub aktivieren).

Security Hub API

Rufen Sie die `EnableSecurityHub`API auf. Wenn Sie Security Hub über die API aktivieren, werden automatisch die folgenden Standardsicherheitsstandards aktiviert:

- Bewährte AWS-Methoden für grundlegende Sicherheit
- Benchmark v1.2.0 der AWS Grundlagen des Center for Internet Security (CIS)

Wenn Sie diese Standards nicht aktivieren möchten, setzen Sie `EnableDefaultStandards` auf `false`.

Sie können den `Tags` Parameter auch verwenden, um der Hub-Ressource Tag-Werte zuzuweisen.

AWS CLI

Führen Sie den Befehl `enable-security-hub` aus. Um die Standardstandards zu aktivieren, schließen Sie ein`--enable-default-standards`. Um die Standardstandards nicht zu aktivieren, fügen Sie hinzu`--no-enable-default-standards`. Die Standardsicherheitsstandards lauten wie folgt:

- Bewährte AWS-Methoden für grundlegende Sicherheit
- Benchmark v1.2.0 der AWS Grundlagen des Center for Internet Security (CIS)

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-
standards | --no-enable-default-standards]
```

Beispiel

```
aws securityhub enable-security-hub --enable-default-standards --tags
 '{"Department": "Security"}'
```

Skript zur Aktivierung mehrerer Konten

> **Note**
>
> Anstelle dieses Skripts empfehlen wir, die zentrale Konfiguration zu verwenden, um Security Hub für mehrere Konten und Regionen zu aktivieren und zu konfigurieren.

Das Security Hub-Skript zur Aktivierung mehrerer Konten in GitHub ermöglicht es Ihnen, Security Hub konto- und regionsübergreifend zu aktivieren. Das Skript automatisiert auch den Prozess des Versendens von Einladungen an Mitgliedskonten und der Aktivierung. AWS Config

Das Skript aktiviert automatisch die Ressourcenaufzeichnung für alle Ressourcen, einschließlich globaler Ressourcen, in allen Regionen. Es beschränkt die Aufzeichnung globaler Ressourcen nicht auf eine einzelne Region.

Es gibt ein entsprechendes Skript, um Security Hub konto- und regionsübergreifend zu deaktivieren.

Nächste Schritte nach der Aktivierung von Security Hub

Nach der Aktivierung von Security Hub empfehlen wir, die Sicherheitsstandards und Sicherheitskontrollen zu aktivieren, die für Ihre Sicherheitsanforderungen wichtig sind. Nachdem Sie die Kontrollen aktiviert haben, beginnt Security Hub mit der Durchführung von Sicherheitsprüfungen und der Generierung von Kontrollergebnissen. Sie können auch Integrationen zwischen Security Hub und anderen AWS-Services Lösungen und Lösungen von Drittanbietern nutzen, um deren Ergebnisse in Security Hub zu sehen.

So funktioniert die zentrale Konfiguration

Die zentrale Konfiguration ist eine Security Hub-Funktion, mit der Sie Security Hub über mehrere Geräte einrichten AWS-Konten und verwalten können AWS-Regionen. Um die zentrale Konfiguration verwenden zu können, müssen Sie zuerst Security Hub und integrieren AWS Organizations. Sie können die Dienste integrieren, indem Sie eine Organisation erstellen und ein delegiertes Security Hub-Administratorkonto für die Organisation festlegen.

Über das delegierte Security Hub-Administratorkonto können Sie angeben, wie der Security Hub Hub-Dienst, die Sicherheitsstandards und die Sicherheitskontrollen in Ihren Unternehmenskonten und Organisationseinheiten (OUs) in allen Regionen konfiguriert werden. Sie können diese Einstellungen in nur wenigen Schritten von einer Hauptregion aus konfigurieren, die als Heimatregion bezeichnet wird. Wenn Sie die zentrale Konfiguration nicht verwenden, müssen Sie Security Hub für jedes Konto und jede Region separat konfigurieren.

Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte Administrator auswählen, welche Konten und Organisationseinheiten konfiguriert werden sollen. Wenn der delegierte Administrator ein Mitgliedskonto oder eine Organisationseinheit als selbstverwaltetes Konto festlegt, kann das Mitglied seine eigenen Einstellungen in jeder Region separat konfigurieren. Wenn der delegierte Administrator ein Mitgliedskonto oder eine Organisationseinheit als zentral verwaltet festlegt, kann nur der delegierte Administrator das Mitgliedskonto oder die Organisationseinheit regionsübergreifend konfigurieren. Sie können alle Konten und Organisationseinheiten in Ihrer Organisation als zentral verwaltet, alle selbstverwaltet oder als eine Kombination aus beidem festlegen.

Um zentral verwaltete Konten zu konfigurieren, verwendet der delegierte Administrator Security Hub Hub-Konfigurationsrichtlinien. Mithilfe von Konfigurationsrichtlinien kann der delegierte Administrator angeben, ob Security Hub aktiviert oder deaktiviert ist und welche Standards und Kontrollen aktiviert und deaktiviert sind. Sie können auch verwendet werden, um die Parameter bestimmter Steuerelemente anzupassen.

Konfigurationsrichtlinien werden in der Heimatregion und allen verknüpften Regionen wirksam. Der delegierte Administrator gibt die Heimatregion der Organisation und die verknüpften Regionen an, bevor er die zentrale Konfiguration verwendet. Der delegierte Administrator kann eine einzige Konfigurationsrichtlinie für die gesamte Organisation oder mehrere Konfigurationsrichtlinien erstellen, um variable Einstellungen für verschiedene Konten und Organisationseinheiten zu konfigurieren.

Dieser Abschnitt bietet einen Überblick über die zentrale Konfiguration.

Vorteile der zentralen Konfiguration

Die zentrale Konfiguration bietet unter anderem folgende Vorteile:

Vereinfachen Sie die Konfiguration des Security Hub Hub-Dienstes und der Funktionen

Wenn Sie die zentrale Konfiguration verwenden, führt Sie Security Hub durch den Prozess der Konfiguration bewährter Sicherheitsmethoden für Ihr Unternehmen. Außerdem werden die daraus resultierenden Konfigurationsrichtlinien automatisch für bestimmte Konten und Organisationseinheiten bereitgestellt. Wenn Sie über bestehende Security Hub Hub-Einstellungen verfügen, z. B. die automatische Aktivierung neuer Sicherheitskontrollen, können Sie diese als Ausgangspunkt für Ihre Konfigurationsrichtlinien verwenden. Darüber hinaus wird auf der Konfigurationsseite der Security Hub Hub-Konsole in Echtzeit eine Zusammenfassung Ihrer Konfigurationsrichtlinien angezeigt. Außerdem wird angezeigt, welche Konten und Organisationseinheiten die einzelnen Richtlinien verwenden.

Konten- und regionsübergreifend konfigurieren

Sie können die zentrale Konfiguration verwenden, um Security Hub für mehrere Konten und Regionen zu konfigurieren. Auf diese Weise können Sie sicherstellen, dass jeder Teil Ihres Unternehmens eine konsistente Konfiguration und einen angemessenen Sicherheitsschutz beibehält.

Passen Sie unterschiedliche Konfigurationen in unterschiedlichen Konten und Organisationseinheiten an

Bei der zentralen Konfiguration können Sie wählen, ob Sie die Konten und Organisationseinheiten Ihres Unternehmens auf unterschiedliche Weise konfigurieren möchten. Beispielsweise können für Ihre Testkonten und Produktionskonten unterschiedliche Konfigurationen erforderlich sein. Sie können auch eine Konfigurationsrichtlinie erstellen, die neue Konten abdeckt, wenn diese der Organisation beitreten.

Vermeiden Sie Konfigurationsabweichungen

Konfigurationsabweichungen treten auf, wenn ein Benutzer eine Änderung an einem Dienst oder einer Funktion vornimmt, die mit den Einstellungen des delegierten Administrators in Konflikt steht. Die zentrale Konfiguration verhindert diese Abweichung. Wenn Sie ein Konto oder eine Organisationseinheit als zentral verwaltet kennzeichnen, kann sie nur vom delegierten Administrator der Organisation konfiguriert werden. Wenn Sie es vorziehen, dass ein bestimmtes Konto oder eine bestimmte Organisationseinheit ihre eigenen Einstellungen konfiguriert, können Sie es als selbstverwaltet kennzeichnen.

Wer sollte die zentrale Konfiguration verwenden?

Die zentrale Konfiguration ist am vorteilhaftesten für AWS Umgebungen, die mehrere Security Hub Hub-Konten enthalten. Es wurde entwickelt, um Ihnen zu helfen, Security Hub für mehrere Konten zentral zu verwalten.

Sie können die zentrale Konfiguration verwenden, um den Security Hub Hub-Dienst, die Sicherheitsstandards und die Sicherheitskontrollen zu konfigurieren. Sie können es auch verwenden, um die Parameter bestimmter Steuerelemente anzupassen. Informationen zu Standards und Kontrollen finden Sie unterSicherheitskontrollen und -standards in AWS Security Hub.

Zentrale Begriffe und Konzepte zur Konfiguration

Wenn Sie die folgenden wichtigen Begriffe und Konzepte verstehen, können Sie die zentrale Konfiguration von Security Hub verwenden.

Zentrale Konfiguration

Eine Security Hub-Funktion, die dem delegierten Security Hub-Administratorkonto für eine Organisation hilft, den Security Hub Hub-Dienst, Sicherheitsstandards und Sicherheitskontrollen für mehrere Konten und Regionen zu konfigurieren. Um diese Einstellungen zu konfigurieren, erstellt und verwaltet der delegierte Administrator Security Hub Hub-Konfigurationsrichtlinien für zentral verwaltete Konten in seiner Organisation. Selbstverwaltete Konten können ihre eigenen Einstellungen in jeder Region separat konfigurieren. Um die zentrale Konfiguration verwenden zu können, müssen Sie Security Hub und integrieren AWS Organizations.

Heimatregion

AWS-Region Von dort aus konfiguriert der delegierte Administrator Security Hub zentral, indem er Konfigurationsrichtlinien erstellt und verwaltet. Konfigurationsrichtlinien gelten in der Heimatregion und allen verknüpften Regionen.

Die Heimatregion dient auch als Security Hub-Aggregationsregion, in der Ergebnisse, Erkenntnisse und andere Daten aus verknüpften Regionen abgerufen werden.

Regionen, die am oder nach dem 20. März 2019 AWS eingeführt wurden, werden als Opt-in-Regionen bezeichnet. Eine Opt-in-Region kann nicht die Heimatregion sein, aber es kann sich um eine verknüpfte Region handeln. Eine Liste der Regionen, für die Sie sich anmelden können, finden Sie im Referenzhandbuch zur AWS Kontoverwaltung unter Überlegungen vor dem Aktivieren und Deaktivieren von Regionen.

Verknüpfte Region

Und AWS-Region das kann von der Heimatregion aus konfiguriert werden. Konfigurationsrichtlinien werden vom delegierten Administrator in der Heimatregion erstellt. Die Richtlinien werden in der Heimatregion und allen verknüpften Regionen wirksam. Sie müssen mindestens eine verknüpfte Region angeben, um die zentrale Konfiguration verwenden zu können.

Eine verknüpfte Region sendet auch Ergebnisse, Erkenntnisse und andere Daten an die Heimatregion.

Regionen, die am oder nach dem 20. März 2019 AWS eingeführt wurden, werden als Opt-in-Regionen bezeichnet. Sie müssen eine solche Region für ein Konto aktivieren, bevor eine Konfigurationsrichtlinie darauf angewendet werden kann. Das Verwaltungskonto für Organizations kann Opt-in-Regionen für ein Mitgliedskonto aktivieren. Weitere Informationen finden Sie im Referenzhandbuch zur Kontoverwaltung unter Geben Sie an, welche Konten für AWS-Regionen Ihr AWS Konto verwendet werden können.

Security Hub Hub-Konfigurationsrichtlinie

Eine Sammlung von Security Hub Hub-Einstellungen, die der delegierte Administrator für zentral verwaltete Konten konfigurieren kann. Dies umfasst:

- Ob Security Hub aktiviert oder deaktiviert werden soll.
- Ob ein oder mehrere Sicherheitsstandards aktiviert werden sollen.
- Welche Sicherheitskontrollen für alle aktivierten Standards aktiviert werden sollen. Der delegierte Administrator kann dies tun, indem er eine Liste bestimmter Steuerelemente bereitstellt, die aktiviert werden sollten, und Security Hub deaktiviert alle anderen Kontrollen (einschließlich neuer Steuerelemente, wenn sie veröffentlicht werden). Alternativ kann der delegierte Administrator eine Liste mit bestimmten Kontrollen bereitstellen, die deaktiviert werden sollten, und Security Hub aktiviert alle anderen Kontrollen (einschließlich neuer Kontrollen, wenn sie veröffentlicht werden).
- Passen Sie optional die Parameter für ausgewählte aktivierte Steuerelemente in allen aktivierten Standards an.

Eine Konfigurationsrichtlinie wird in der Heimatregion und allen verknüpften Regionen wirksam, nachdem sie mindestens einem Konto, einer Organisationseinheit (OU) oder dem Stammverzeichnis zugeordnet wurde.

Auf der Security Hub-Konsole kann der delegierte Administrator die von Security Hub empfohlene Konfigurationsrichtlinie auswählen oder benutzerdefinierte Konfigurationsrichtlinien erstellen. Mit der Security Hub Hub-API und AWS CLI kann der delegierte Administrator nur benutzerdefinierte Konfigurationsrichtlinien erstellen. Der delegierte Administrator kann maximal 20 benutzerdefinierte Konfigurationsrichtlinien erstellen.

In der empfohlenen Konfigurationsrichtlinie sind Security Hub, der Standard AWS Foundation Security Best Practices (FSBP) und alle vorhandenen und neuen FSBP-Steuerelemente aktiviert. Steuerelemente, die Parameter akzeptieren, verwenden die Standardwerte. Die empfohlene Konfigurationsrichtlinie gilt für die gesamte Organisation.

Um unterschiedliche Einstellungen auf die Organisation anzuwenden oder unterschiedliche Konfigurationsrichtlinien auf verschiedene Konten und Organisationseinheiten anzuwenden, erstellen Sie eine benutzerdefinierte Konfigurationsrichtlinie.

Lokale Konfiguration

Der Standardkonfigurationstyp für eine Organisation nach der Integration von Security Hub und AWS Organizations. Bei der lokalen Konfiguration kann der delegierte Administrator festlegen, dass Security Hub und Standardsicherheitsstandards in neuen Unternehmenskonten in der aktuellen Region automatisch aktiviert werden. Wenn der delegierte Administrator die Standardstandards automatisch aktiviert, werden alle Steuerelemente, die Teil dieser Standards sind, auch automatisch mit Standardparametern für neue Organisationskonten aktiviert. Diese Einstellungen gelten nicht für bestehende Konten, sodass es nach dem Beitritt eines Kontos zur Organisation zu Konfigurationsabweichungen kommen kann. Die Deaktivierung bestimmter Kontrollen, die Teil der Standardstandards sind, und die Konfiguration zusätzlicher Standards und Kontrollen müssen für jedes Konto und jede Region separat erfolgen.

Die lokale Konfiguration unterstützt die Verwendung von Konfigurationsrichtlinien nicht. Um Konfigurationsrichtlinien zu verwenden, müssen Sie zur zentralen Konfiguration wechseln.

Manuelle Kontoverwaltung

Wenn Sie Security Hub nicht in Security Hub integrieren AWS Organizations oder ein eigenständiges Konto haben, müssen Sie die Einstellungen für jedes Konto in jeder Region separat angeben. Die manuelle Kontoverwaltung unterstützt die Verwendung von Konfigurationsrichtlinien nicht.

Zentrale Konfigurations-APIs

Security Hub-Operationen, die nur der vom Security Hub delegierte Security Hub-Administrator in der Heimatregion verwenden kann, um Konfigurationsrichtlinien für zentral verwaltete Konten zu verwalten. Zu den Vorgängen gehören:

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

Kontospezifische APIs

Security Hub-Operationen, die verwendet werden können, um Security Hub, Standards und Kontrollen auf einer bestimmten account-by-account Basis zu aktivieren oder zu deaktivieren. Diese Operationen werden in jeder einzelnen Region verwendet.

Selbstverwaltete Konten können kontospezifische Operationen verwenden, um ihre eigenen Einstellungen zu konfigurieren. Zentral verwaltete Konten können die folgenden kontospezifischen Vorgänge in der Heimatregion und verknüpften Regionen nicht verwenden. In diesen Regionen kann nur der delegierte Administrator zentral verwaltete Konten über zentrale Konfigurationsvorgänge und Konfigurationsrichtlinien konfigurieren.

- `BatchDisableStandards`
- `BatchEnableStandards`
- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`
- `EnableSecurityHub`
- `UpdateStandardsControl`

Um den Kontostatus zu überprüfen, kann der Besitzer eines zentral verwalteten Kontos `Get` beliebige `Describe` Operationen der Security Hub Hub-API verwenden.

Wenn Sie statt der zentralen Konfiguration die lokale Konfiguration oder die manuelle Kontoverwaltung verwenden, können Sie diese kontospezifischen Operationen verwenden.

Selbstverwaltete Konten können auch AND-Operationen verwenden`*Invitations`. `*Members` Wir empfehlen jedoch, dass selbstverwaltete Konten diese Operationen nicht verwenden. Richtlinienzuordnungen können fehlschlagen, wenn ein Mitgliedskonto eigene Mitglieder hat, die Teil einer anderen Organisation sind als die des delegierten Administrators.

Organisationseinheit (OU)

In AWS Organizations und Security Hub, ein Container für eine Gruppe von AWS-Konten. Eine Organisationseinheit (OU) kann auch andere Organisationseinheiten enthalten, sodass Sie eine Hierarchie erstellen können, die einem umgedrehten Baum ähnelt, mit einer übergeordneten Organisationseinheit an der Spitze und Zweigen von Organisationseinheiten, die nach unten reichen und in Konten enden, die Blätter des Baums sind. Eine Organisationseinheit kann genau eine übergeordnete Organisationseinheit haben, und jedes Organisationskonto kann Mitglied genau einer Organisationseinheit sein.

Sie können Organisationseinheiten in AWS Organizations oder verwalten AWS Control Tower. Weitere Informationen finden Sie unter Verwaltung von Organisationseinheiten im AWS Organizations Benutzerhandbuch oder Verwaltung von Organisationen und Konten mit AWS Control Tower im AWS Control Tower Benutzerhandbuch.

Der delegierte Administrator kann Konfigurationsrichtlinien bestimmten Konten oder Organisationseinheiten oder dem Stamm zuordnen, sodass alle Konten und Organisationseinheiten in einer Organisation abgedeckt werden.

Zentral verwaltet

Ein Konto, eine Organisationseinheit oder ein Stammkonto, das nur der delegierte Administrator mithilfe von Konfigurationsrichtlinien regionsübergreifend konfigurieren kann.

Das delegierte Administratorkonto gibt an, ob ein Konto zentral verwaltet wird. Der delegierte Administrator kann auch den Status eines Kontos von zentral verwaltet in selbstverwaltet ändern oder umgekehrt.

Selbstverwaltet

Ein Konto, eine Organisationseinheit oder ein Root-Konto, das seine eigenen Security Hub Hub-Einstellungen verwaltet. Ein selbstverwaltetes Konto verwendet kontospezifische Operationen, um Security Hub für sich selbst in jeder Region separat zu konfigurieren. Dies steht im Gegensatz

zu zentral verwalteten Konten, die nur vom delegierten Administrator regionsübergreifend über Konfigurationsrichtlinien konfiguriert werden können.

Das delegierte Administratorkonto gibt an, ob es sich um ein selbstverwaltetes Konto handelt. Das delegierte Administratorkonto kann auch den Status eines Kontos von selbstverwaltet in zentral verwaltet ändern oder umgekehrt.

Der delegierte Administrator kann selbstverwaltetes Verhalten auf ein Konto oder eine Organisationseinheit anwenden. Alternativ kann ein Konto oder eine Organisationseinheit das selbstverwaltete Verhalten von einem Elternteil erben. Das delegierte Administratorkonto kann selbst ein selbstverwaltetes Konto sein.

Zuordnung der Konfigurationsrichtlinien

Eine Verknüpfung zwischen einer Konfigurationsrichtlinie und einem Konto, einer Organisationseinheit (OU) oder einem Stamm. Wenn eine Richtlinienzuordnung vorhanden ist, verwendet das Konto, die Organisationseinheit oder das Stammverzeichnis die in der Konfigurationsrichtlinie definierten Einstellungen. In einem der folgenden Fälle besteht eine Zuordnung:

- Wenn der delegierte Administrator eine Konfigurationsrichtlinie direkt auf ein Konto, eine Organisationseinheit oder einen Root-Benutzer anwendet
- Wenn ein Konto oder eine Organisationseinheit eine Konfigurationsrichtlinie von einer übergeordneten Organisationseinheit oder der Stammorganisation erbt

Eine Zuordnung besteht, bis eine andere Konfiguration angewendet oder vererbt wird.

Angewendete Konfigurationsrichtlinie

Eine Art von Zuordnung von Konfigurationsrichtlinien, bei der der delegierte Administrator eine Konfigurationsrichtlinie direkt auf Zielkonten, Organisationseinheiten oder das Stammkonto anwendet. Ziele werden so konfiguriert, wie sie in der Konfigurationsrichtlinie definiert sind, und nur der delegierte Administrator kann ihre Konfiguration ändern. Wenn die Konfigurationsrichtlinie auf das Stammverzeichnis angewendet wird, wirkt sie sich auf alle Konten und Organisationseinheiten in der Organisation aus, die keine andere Konfiguration aufgrund von Anwendungen oder Vererbung durch das nächstgelegene übergeordnete Unternehmen verwenden.

Der delegierte Administrator kann eine selbstverwaltete Konfiguration auch auf bestimmte Konten, Organisationseinheiten oder das Stammverzeichnis anwenden.

Geerbte Konfigurationsrichtlinie

Eine Art von Zuordnung von Konfigurationsrichtlinien, bei der ein Konto oder eine Organisationseinheit die Konfiguration der nächstgelegenen übergeordneten Organisationseinheit oder der Stammorganisation übernimmt. Wenn eine Konfigurationsrichtlinie nicht direkt auf ein Konto oder eine Organisationseinheit angewendet wird, erbt sie die Konfiguration der nächstgelegenen übergeordneten Organisation. Alle Elemente einer Richtlinie werden vererbt. Mit anderen Worten, ein Konto oder eine Organisationseinheit kann sich nicht dafür entscheiden, selektiv nur Teile einer Richtlinie zu erben. Wenn der nächstgelegene Elternteil selbst verwaltet wird, erbt das untergeordnete Konto oder die Organisationseinheit das selbstverwaltete Verhalten des Elternteils.

Die Vererbung kann eine angewendete Konfiguration nicht außer Kraft setzen. Das heißt, wenn eine Konfigurationsrichtlinie oder eine selbstverwaltete Konfiguration direkt auf ein Konto oder eine Organisationseinheit angewendet wird, verwendet sie diese Konfiguration und erbt nicht die Konfiguration der übergeordneten Einheit.

Root

In AWS Organizations und Security Hub, dem übergeordneten Knoten der obersten Ebene in einer Organisation. Wenn der delegierte Administrator eine Konfigurationsrichtlinie auf Root anwendet, wird die Richtlinie allen Konten und Organisationseinheiten in der Organisation zugeordnet, es sei denn, sie verwenden aufgrund von Anwendung oder Vererbung eine andere Richtlinie oder sind als selbstverwaltet gekennzeichnet. Wenn der Administrator das Stammverzeichnis als selbstverwaltet festlegt, werden alle Konten und Organisationseinheiten in der Organisation selbst verwaltet, es sei denn, sie verwenden eine Konfigurationsrichtlinie durch Anwendung oder Vererbung. Wenn das Stammverzeichnis selbst verwaltet wird und derzeit keine Konfigurationsrichtlinien existieren, behalten alle neuen Konten in der Organisation ihre aktuellen Einstellungen bei.

Neue Konten, die einer Organisation beitreten, fallen unter das Stammkonto, bis sie einer bestimmten Organisationseinheit zugewiesen werden. Wenn ein neues Konto keiner Organisationseinheit zugewiesen ist, erbt es die Stammkonfiguration, es sei denn, der delegierte Administrator bestimmt es als selbstverwaltetes Konto.

Beginnen Sie mit der zentralen Konfiguration

Das AWS Security Hub delegierte Administratorkonto kann die zentrale Konfiguration verwenden, um Security Hub, Standards und Kontrollen für mehrere Konten und Organisationseinheiten (OUs) zu konfigurieren. AWS-Regionen

In diesem Abschnitt werden die Voraussetzungen für die zentrale Konfiguration und die ersten Schritte zur Verwendung dieser Konfiguration erläutert.

Voraussetzungen für die zentrale Konfiguration

Bevor Sie die zentrale Konfiguration verwenden können, müssen Sie Security Hub in eine Heimatregion integrieren AWS Organizations und eine Heimatregion festlegen. Wenn Sie die Security Hub Hub-Konsole verwenden, sind diese Voraussetzungen im Opt-in-Workflow für die zentrale Konfiguration enthalten.

Integrieren Sie sich mit Organizations

Sie müssen Security Hub und Organizations integrieren, um die zentrale Konfiguration verwenden zu können.

Um diese Dienste zu integrieren, erstellen Sie zunächst eine Organisation in Organizations. Über das Verwaltungskonto der Organizations bestimmen Sie dann ein delegiertes Security Hub-Administratorkonto. Anweisungen finden Sie unter Integrieren von Security Hub mit AWS Organizations.

Stellen Sie sicher, dass Sie Ihren delegierten Administrator in Ihrer gewünschten Heimatregion angeben. Wenn Sie die zentrale Konfiguration verwenden, wird derselbe delegierte Administrator automatisch auch in allen verknüpften Regionen eingerichtet. Das Verwaltungskonto für Organizations kann nicht als delegiertes Administratorkonto festgelegt werden.

> **Important**
>
> Wenn Sie die zentrale Konfiguration verwenden, können Sie die Security Hub-Konsole oder die Security Hub-APIs nicht verwenden, um das delegierte Administratorkonto zu ändern oder zu entfernen. Wenn das Verwaltungskonto der Organizations AWS Organizations APIs verwendet, um den delegierten Security Hub-Administrator zu ändern oder zu entfernen, stoppt Security Hub automatisch die zentrale Konfiguration. Ihre Konfigurationsrichtlinien

werden ebenfalls getrennt und gelöscht. Mitgliedskonten behalten die Konfiguration bei, die sie hatten, bevor der delegierte Administrator geändert oder entfernt wurde.

Geben Sie eine Heimatregion an

Sie müssen eine Heimatregion angeben, um die zentrale Konfiguration verwenden zu können. Die Heimatregion ist die Region, von der aus der delegierte Administrator die Organisation konfiguriert.

Um die zentrale Konfiguration zu verwenden, müssen Sie mindestens eine verknüpfte Region angeben, die von der Heimatregion aus konfiguriert werden kann.

> **Note**
>
> Bei der Heimatregion kann es sich nicht um eine Region handeln, die als Opt-in-Region ausgewiesen AWS wurde. Eine Opt-in-Region ist standardmäßig deaktiviert. Eine Liste der Opt-in-Regionen finden Sie unter Überlegungen vor der Aktivierung und Deaktivierung von Regionen im Referenzhandbuch zur AWSKontoverwaltung.

Der delegierte Administrator kann Konfigurationsrichtlinien nur von der Heimatregion aus erstellen und verwalten. Konfigurationsrichtlinien werden in der Heimatregion und allen verknüpften Regionen wirksam. Sie können keine Konfigurationsrichtlinie erstellen, die nur für eine Teilmenge dieser Regionen gilt und nicht für andere.

Die Heimatregion ist auch Ihre Security Hub-Aggregationsregion, die Ergebnisse, Erkenntnisse und andere Daten aus verknüpften Regionen erhält.

Wenn Sie bereits eine Aggregationsregion für die regionsübergreifende Aggregation festgelegt haben, ist dies Ihre Standard-Heimatregion für die zentrale Konfiguration. Sie können die Heimatregion ändern, bevor Sie die zentrale Konfiguration verwenden, indem Sie Ihren aktuellen Suchaggregator löschen und einen neuen in der gewünschten Heimatregion erstellen. Ein Findingaggregator ist eine Security Hub Hub-Ressource, die die Heimatregion und verknüpfte Regionen spezifiziert.

Um eine Heimatregion festzulegen, folgen Sie den Schritten zum Einstellen einer Aggregationsregion. Wenn Sie bereits eine Heimatregion haben, können Sie die GetFindingAggregatorAPI aufrufen, um Details zu dieser Region zu sehen, einschließlich der Regionen, die derzeit damit verknüpft sind.

Starten Sie die zentrale Konfiguration

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um mit der Verwendung der zentralen Konfiguration für Ihr Unternehmen zu beginnen.

Security Hub console

Um Ihre Organisation zentral zu konfigurieren

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus. Wählen Sie dann Zentrale Konfiguration starten aus.

   Wenn Sie bei Security Hub einsteigen, wählen Sie Gehe zu Security Hub.
3. Wählen Sie auf der Seite Delegierten Administrator benennen Ihr delegiertes Administratorkonto aus oder geben Sie dessen Konto-ID ein. Falls zutreffend, empfehlen wir, denselben delegierten Administrator zu wählen, den Sie für andere AWS Sicherheits- und Compliance-Dienste eingerichtet haben. Wählen Sie Als delegierten Administrator festlegen aus.
4. Wählen Sie auf der Seite Organisation zentralisieren im Abschnitt Regionen Ihre Heimatregion aus. Sie müssen in der Heimatregion angemeldet sein, um fortzufahren. Wenn Sie bereits eine Aggregationsregion für die regionsübergreifende Aggregation festgelegt haben, wird diese als Heimatregion angezeigt. Um die Heimatregion zu ändern, wählen Sie „Regionseinstellungen bearbeiten“. Sie können dann Ihre bevorzugte Heimatregion auswählen und zu diesem Workflow zurückkehren.
5. Wählen Sie mindestens eine Region aus, um eine Verknüpfung mit der Heimatregion herzustellen. Wählen Sie optional aus, ob Sie future unterstützte Regionen automatisch mit der Heimatregion verknüpfen möchten. Die Regionen, die Sie hier auswählen, werden vom delegierten Administrator von der Heimatregion aus konfiguriert. Die Konfigurationsrichtlinien gelten in Ihrer Heimatregion und allen verknüpften Regionen.
6. Wählen Sie Bestätigen und fortfahren.
7. Sie können jetzt die zentrale Konfiguration verwenden. Folgen Sie weiterhin den Anweisungen der Konsole, um Ihre erste Konfigurationsrichtlinie zu erstellen. Wenn Sie noch nicht bereit sind, eine Konfigurationsrichtlinie zu erstellen, wählen Sie Ich bin noch nicht bereit zur Konfiguration. Sie können später eine Richtlinie erstellen, indem Sie im Navigationsbereich Einstellungen und Konfiguration auswählen. Anweisungen zum Erstellen

einer Konfigurationsrichtlinie finden Sie unterSecurity Hub Hub-Konfigurationsrichtlinien erstellen und zuordnen.

Security Hub API

Um Security Hub zentral zu konfigurieren

1. Rufen Sie die UpdateOrganizationConfigurationAPI mit den Anmeldeinformationen des delegierten Administratorkontos von der Heimatregion aus auf.
2. Stellen Sie das `AutoEnable` Feld auf ein. `false`
3. Stellen Sie das `ConfigurationType` Feld im `OrganizationConfiguration` Objekt auf ein`CENTRAL`. Diese Aktion hat folgende Auswirkungen:
   - Legt das anrufende Konto in allen verknüpften Regionen als delegierten Security Hub-Administrator fest.
   - Aktiviert Security Hub im delegierten Administratorkonto in allen verknüpften Regionen.
   - Benennt das anrufende Konto als delegierten Security Hub-Administrator für neue und bestehende Konten, die Security Hub verwenden und zur Organisation gehören. Dies geschieht in der Heimatregion und allen verknüpften Regionen. Das anrufende Konto wird nur dann als delegierter Administrator für neue Organisationskonten eingerichtet, wenn sie einer Konfigurationsrichtlinie zugeordnet sind, für die Security Hub aktiviert ist. Das anrufende Konto wird nur dann als delegierter Administrator für bestehende Organisationskonten eingerichtet, wenn Security Hub für diese bereits aktiviert ist.
   - Stellt AutoEnable`false`in allen verknüpften Regionen und AutoEnableStandardsauf `NONE` in der Heimatregion und allen verknüpften Regionen ein. Diese Parameter sind in der Startseite und den verknüpften Regionen nicht relevant, wenn Sie die zentrale Konfiguration verwenden, aber Sie können Security Hub und Standardsicherheitsstandards in Organisationskonten mithilfe von Konfigurationsrichtlinien automatisch aktivieren.
4. Sie können jetzt die zentrale Konfiguration verwenden. Der delegierte Administrator kann Konfigurationsrichtlinien erstellen, um Security Hub in Ihrer Organisation zu konfigurieren. Anweisungen zum Erstellen einer Konfigurationsrichtlinie finden Sie unterSecurity Hub Hub-Konfigurationsrichtlinien erstellen und zuordnen.

Beispiel für eine API-Anfrage:

```
{
```

```
    "AutoEnable": false,
    "OrganizationConfiguration": {
        "ConfigurationType": "CENTRAL"
    }
}
```

AWS CLI

Um Security Hub zentral zu konfigurieren

1. Führen Sie den update-organization-configurationBefehl mit den Anmeldeinformationen des delegierten Administratorkontos in der Heimatregion aus.
2. Schließen Sie den Parameter `no-auto-enable` ein.
3. Stellen Sie das `ConfigurationType` Feld im `organization-configuration` Objekt auf `CENTRAL` ein. Diese Aktion hat folgende Auswirkungen:
   - Legt das anrufende Konto in allen verknüpften Regionen als delegierten Security Hub-Administrator fest.
   - Aktiviert Security Hub im delegierten Administratorkonto in allen verknüpften Regionen.
   - Benennt das anrufende Konto als delegierten Security Hub-Administrator für neue und bestehende Konten, die Security Hub verwenden und zur Organisation gehören. Dies geschieht in der Heimatregion und allen verknüpften Regionen. Das anrufende Konto wird nur dann als delegierter Administrator für neue Organisationskonten eingerichtet, wenn sie einer Konfigurationsrichtlinie zugeordnet sind, für die Security Hub aktiviert ist. Das anrufende Konto wird nur dann als delegierter Administrator für bestehende Organisationskonten eingerichtet, wenn Security Hub für diese bereits aktiviert ist.
   - Legt die Option zur automatischen Aktivierung no-auto-enablein allen verknüpften Regionen und auf `NONE` in der Heimatregion und allen verknüpften Regionen fest auto-enable-standards. Diese Parameter sind in der Startseite und den verknüpften Regionen nicht relevant, wenn Sie die zentrale Konfiguration verwenden, aber Sie können Security Hub und Standardsicherheitsstandards in Organisationskonten mithilfe von Konfigurationsrichtlinien automatisch aktivieren.
4. Sie können jetzt die zentrale Konfiguration verwenden. Der delegierte Administrator kann Konfigurationsrichtlinien erstellen, um Security Hub in Ihrer Organisation zu konfigurieren. Anweisungen zum Erstellen einer Konfigurationsrichtlinie finden Sie unterSecurity Hub Hub-Konfigurationsrichtlinien erstellen und zuordnen.

Beispielbefehl:

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}'
```

Auswahl des Verwaltungstyps von Konten und Organisationseinheiten

Wenn Sie die zentrale Konfiguration verwenden, kann der AWS Security Hub delegierte Administrator jedes Organisationskonto und jede Organisationseinheit (OU) als zentral verwaltet oder selbstverwaltet festlegen. Der Verwaltungstyp eines Kontos oder einer Organisationseinheit bestimmt, wie Sie die Security Hub Hub-Einstellungen angeben und ändern können.

Ein selbstverwaltetes Konto oder eine Organisationseinheit kann ihre eigenen Security Hub Hub-Einstellungen in jedem AWS-Region Konto separat konfigurieren. Der delegierte Administrator kann Security Hub Hub-Einstellungen für ein selbstverwaltetes Konto oder eine selbstverwaltete Organisationseinheit nicht konfigurieren, und ihnen können keine Konfigurationsrichtlinien zugeordnet werden. Im Gegensatz dazu kann nur der delegierte Administrator die Security Hub Hub-Einstellungen für zentral verwaltete Konten und Organisationseinheiten in der Heimatregion und den verknüpften Regionen konfigurieren. Konfigurationsrichtlinien können zentral verwalteten Konten und Organisationseinheiten zugeordnet werden.

Der delegierte Administrator kann den Status eines Kontos oder einer Organisationseinheit zwischen selbstverwalteten und zentral verwalteten Konten ändern. Standardmäßig werden alle Konten und Organisationseinheiten selbst verwaltet, wenn Sie die zentrale Konfiguration über die Security Hub Hub-API starten. In der Konsole hängt der Verwaltungstyp von Ihrer ersten Konfigurationsrichtlinie ab. Konten und Organisationseinheiten, die Sie Ihrer ersten Richtlinie zuordnen, werden zentral verwaltet. Andere Konten und Organisationseinheiten werden standardmäßig selbst verwaltet.

Wenn Sie einem selbstverwalteten Konto eine Konfigurationsrichtlinie zuordnen, hat die Richtlinie Vorrang vor der Bezeichnung für selbstverwaltetes Konto. Das Konto wird zentral verwaltet und übernimmt die Einstellungen, die in der Konfigurationsrichtlinie enthalten sind.

Untergeordnete Konten und Organisationseinheiten können das selbstverwaltete Verhalten von einer selbstverwalteten übergeordneten Person erben, genauso wie untergeordnete Konten und

Organisationseinheiten Konfigurationsrichtlinien von einer zentral verwalteten übergeordneten Einheit erben können. Weitere Informationen finden Sie unter Richtlinienverknüpfung durch Anwendung und Vererbung.

Ein selbstverwaltetes Konto oder eine Organisationseinheit kann keine Konfigurationsrichtlinie von einem übergeordneten Knoten oder vom Stammknoten erben. Wenn Sie beispielsweise möchten, dass alle Konten und Organisationseinheiten in Ihrer Organisation eine Konfigurationsrichtlinie vom Stammverzeichnis erben, müssen Sie den Verwaltungstyp für selbstverwaltete Knoten auf zentral verwaltete Knoten ändern.

Angeben von Einstellungen für selbstverwaltete Konten

Selbstverwaltete Konten müssen ihre eigenen Einstellungen in jeder Region separat konfigurieren.

Besitzer von selbstverwalteten Konten können die folgenden Operationen der Security Hub Hub-API in jeder Region aufrufen, um ihre Einstellungen zu konfigurieren:

- `EnableSecurityHub`und `DisableSecurityHub` um den Security Hub Hub-Dienst zu aktivieren oder zu deaktivieren
- `BatchEnableStandards`und `BatchDisableStandards` um Standards zu aktivieren oder zu deaktivieren
- `BatchUpdateStandardsControlAssociations`oder `UpdateStandardsControl` um Steuerungen zu aktivieren oder zu deaktivieren

Selbstverwaltete Konten können auch `*Invitations` `*Members` AND-Operationen verwenden. Wir empfehlen jedoch, dass selbstverwaltete Konten diese Operationen nicht verwenden. Richtlinienzuordnungen können fehlschlagen, wenn ein Mitgliedskonto eigene Mitglieder hat, die Teil einer anderen Organisation sind als die des delegierten Administrators.

Eine Beschreibung der API-Aktionen von Security Hub finden Sie in der AWS Security Hub API-Referenz.

Selbstverwaltete Konten können auch die Security Hub Hub-Konsole verwenden oder AWS CLI ihre Einstellungen in jeder Region konfigurieren.

Selbstverwaltete Konten können keine APIs aufrufen, die sich auf Security Hub Hub-Konfigurationsrichtlinien und Richtlinienzuordnungen beziehen. Nur der delegierte Administrator kann zentrale Konfigurations-APIs aufrufen und Konfigurationsrichtlinien verwenden, um zentral verwaltete Konten zu konfigurieren.

Auswahl des Verwaltungstyps von Konten und Organisationseinheiten

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um ein Konto oder eine Organisationseinheit als zentral verwaltet oder selbstverwaltet zu kennzeichnen.

Security Hub console

Um den Verwaltungstyp eines Kontos oder einer Organisationseinheit auszuwählen

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub-Administratorkontos in der Heimatregion an.
2. Wählen Sie Konfiguration.
3. Wählen Sie auf der Registerkarte Organisation das Zielkonto oder die Organisationseinheit aus. Wählen Sie Bearbeiten aus.
4. Wählen Sie auf der Seite Konfiguration definieren als Verwaltungstyp die Option Zentral verwaltet aus, wenn der delegierte Administrator das Zielkonto oder die Organisationseinheit konfigurieren soll. Wählen Sie dann „Spezifische Richtlinie anwenden“ aus, wenn Sie dem Ziel eine bestehende Konfigurationsrichtlinie zuordnen möchten. Wählen Sie Von meiner Organisation übernehmen, wenn Sie möchten, dass das Ziel die Konfiguration seines engsten übergeordneten Unternehmens erbt. Wählen Sie Selbstverwaltet, wenn Sie möchten, dass das Konto oder die Organisationseinheit ihre eigenen Einstellungen konfiguriert.
5. Wählen Sie Weiter aus. Überprüfen Sie Ihre Änderungen und wählen Sie Speichern.

Security Hub API

Um den Verwaltungstyp eines Kontos oder einer Organisationseinheit auszuwählen

1. Rufen Sie die StartConfigurationPolicyAssociationAPI über das delegierte Security Hub-Administratorkonto in der Heimatregion auf.
2. Geben Sie für das `ConfigurationPolicyIdentifier` Feld an, `SELF_MANAGED_SECURITY_HUB` ob das Konto oder die Organisationseinheit ihre eigenen Einstellungen steuern soll. Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der entsprechenden Konfigurationsrichtlinie an, wenn Sie möchten, dass der delegierte Administrator die Einstellungen für das Konto oder die Organisationseinheit steuert.

3. Geben Sie für das `Target` Feld die AWS-Konto ID, OU-ID oder Root-ID des Ziels ein, dessen Verwaltungstyp Sie ändern möchten. Dadurch wird das selbstverwaltete Verhalten oder die angegebene Konfigurationsrichtlinie dem Ziel zugeordnet. Untergeordnete Konten des Ziels erben möglicherweise die selbstverwaltete Verhaltens- oder Konfigurationsrichtlinie.

Beispiel für eine API-Anfrage zur Benennung eines selbstverwalteten Kontos:

```
{
    "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Um den Verwaltungstyp eines Kontos oder einer Organisationseinheit auszuwählen

1. Führen Sie den start-configuration-policy-associationBefehl über das delegierte Security Hub-Administratorkonto in der Heimatregion aus.
2. Geben Sie `configuration-policy-identifier` im Feld an, `SELF_MANAGED_SECURITY_HUB` ob das Konto oder die Organisationseinheit ihre eigenen Einstellungen steuern soll. Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der entsprechenden Konfigurationsrichtlinie an, wenn Sie möchten, dass der delegierte Administrator die Einstellungen für das Konto oder die Organisationseinheit steuert.
3. Geben Sie für das `target` Feld die AWS-Konto ID, OU-ID oder Root-ID des Ziels ein, dessen Verwaltungstyp Sie ändern möchten. Dadurch wird das selbstverwaltete Verhalten oder die angegebene Konfigurationsrichtlinie dem Ziel zugeordnet. Untergeordnete Konten des Ziels erben möglicherweise die selbstverwaltete Verhaltens- oder Konfigurationsrichtlinie.

Beispielbefehl zur Benennung eines selbstverwalteten Kontos:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

So funktionieren die Security Hub Hub-Konfigurationsrichtlinien

Das delegierte Administratorkonto kann AWS Security Hub Konfigurationsrichtlinien erstellen, um Security Hub, Sicherheitsstandards und Sicherheitskontrollen in Ihrer Organisation zu konfigurieren. Nach der Erstellung einer Konfigurationsrichtlinie kann der delegierte Administrator sie Konten, Organisationseinheiten (OUs) oder dem Stamm zuordnen. Der delegierte Administrator kann auch Konfigurationsrichtlinien anzeigen, bearbeiten oder löschen.

Überlegungen zu Richtlinien

Bevor Sie eine Konfigurationsrichtlinie in Security Hub erstellen, sollten Sie die folgenden Details berücksichtigen.

- Konfigurationsrichtlinien müssen verknüpft werden, damit sie wirksam werden. Nachdem Sie eine Konfigurationsrichtlinie erstellt haben, können Sie sie einem oder mehreren Konten, Organisationseinheiten (OUs) oder dem Stamm zuordnen. Eine Konfigurationsrichtlinie kann Konten oder Organisationseinheiten direkt oder durch Vererbung von einer übergeordneten Organisationseinheit zugeordnet werden.
- Ein Konto oder eine Organisationseinheit kann nur einer Konfigurationsrichtlinie zugeordnet werden. Um widersprüchliche Einstellungen zu vermeiden, kann ein Konto oder eine Organisationseinheit jeweils nur einer Konfigurationsrichtlinie zugeordnet werden. Alternativ kann ein Konto oder eine Organisationseinheit selbst verwaltet werden.
- Die Konfigurationsrichtlinien sind vollständig — Die Konfigurationsrichtlinien bieten eine vollständige Spezifikation der Einstellungen. Beispielsweise kann ein Kinderkonto keine Einstellungen für einige Steuerelemente aus einer Richtlinie und Einstellungen für andere Steuerelemente aus einer anderen Richtlinie akzeptieren. Wenn Sie eine Richtlinie einem Kinderkonto zuordnen, stellen Sie sicher, dass die Richtlinie alle Einstellungen festlegt, die das Kinderkonto verwenden soll.
- Konfigurationsrichtlinien können nicht rückgängig gemacht werden — Es gibt keine Möglichkeit, eine Konfigurationsrichtlinie rückgängig zu machen, nachdem Sie sie Konten oder Organisationseinheiten zugeordnet haben. Wenn Sie beispielsweise eine Konfigurationsrichtlinie, die CloudWatch Steuerelemente deaktiviert, einem bestimmten Konto zuordnen und diese Richtlinie dann aufheben, sind die CloudWatch Steuerelemente in diesem Konto weiterhin deaktiviert. Um die CloudWatch Kontrollen wieder zu aktivieren, können Sie das Konto einer neuen Richtlinie zuordnen, die die Kontrollen aktiviert. Alternativ können Sie das Konto auf Selbstverwaltung umstellen und alle CloudWatch Steuerelemente im Konto aktivieren.

- Konfigurationsrichtlinien gelten in Ihrer Heimatregion und allen verknüpften Regionen — Eine Konfigurationsrichtlinie wirkt sich auf alle zugehörigen Konten in der Heimatregion und auf alle verknüpften Regionen aus. Sie können keine Konfigurationsrichtlinie erstellen, die nur in einigen dieser Regionen wirksam ist und in anderen nicht. Eine Ausnahme bilden Kontrollen, die globale Ressourcen betreffen.

  Regionen, die am oder nach dem 20. März 2019 AWS eingeführt wurden, werden als Opt-in-Regionen bezeichnet. Sie müssen eine solche Region für ein Konto aktivieren, bevor dort eine Konfigurationsrichtlinie wirksam wird. Das Verwaltungskonto für Organizations kann Opt-in-Regionen für ein Mitgliedskonto aktivieren. Anweisungen zur Aktivierung von Opt-in-Regionen finden Sie im Referenzhandbuch zur Kontoverwaltung unter Geben Sie an, welche Regionen für AWS-Regionen Ihr AWS Konto verwendet werden können.

  Wenn Ihre Richtlinie ein Steuerelement konfiguriert, das in der Heimatregion oder einer oder mehreren verknüpften Regionen nicht verfügbar ist, überspringt Security Hub die Kontrollkonfiguration in nicht verfügbaren Regionen, wendet die Konfiguration jedoch in Regionen an, in denen das Steuerelement verfügbar ist.
- Konfigurationsrichtlinien sind Ressourcen — Als Ressource hat eine Konfigurationsrichtlinie einen Amazon-Ressourcennamen (ARN) und eine Universally Unique Identifier (UUID). Der ARN verwendet das folgende Format:`arn:`*`partition:`*`securityhub:`*`region`*`:`*`delegated administrator account ID`*`:configuration-policy/`*`configuration policy UUID`*. Eine selbstverwaltete Konfiguration hat keinen ARN oder UUID. Der Bezeichner für eine selbstverwaltete Konfiguration lautet. `SELF_MANAGED_SECURITY_HUB`

Arten von Konfigurationsrichtlinien

Jede Konfigurationsrichtlinie legt die folgenden Einstellungen fest:

- Aktivieren oder deaktivieren Sie Security Hub.
- Aktivieren Sie einen oder mehrere Sicherheitsstandards.
- Geben Sie an, welche Sicherheitskontrollen für alle aktivierten Standards aktiviert sind. Sie können dies tun, indem Sie eine Liste bestimmter Steuerelemente bereitstellen, die aktiviert werden sollten, und Security Hub deaktiviert alle anderen Steuerelemente, einschließlich neuer Steuerelemente, wenn sie veröffentlicht werden. Alternativ können Sie eine Liste mit bestimmten Steuerelementen bereitstellen, die deaktiviert werden sollten, und Security Hub aktiviert alle anderen Kontrollen, einschließlich neuer Steuerelemente, wenn sie veröffentlicht werden.

- Passen Sie optional die Parameter für ausgewählte aktivierte Steuerelemente für alle aktivierten Standards an.

Zentrale Konfigurationsrichtlinien beinhalten keine AWS Config Rekordereinstellungen. Sie müssen die Aufzeichnung für die erforderlichen Ressourcen separat aktivieren AWS Config und einschalten, damit Security Hub Kontrollergebnisse generieren kann. Weitere Informationen finden Sie unter Konfiguration AWS Config.

Wenn Sie die zentrale Konfiguration verwenden, deaktiviert Security Hub automatisch Steuerungen, die globale Ressourcen in allen Regionen außer der Heimatregion betreffen. Andere Steuerelemente, die Sie über eine Konfigurationsrichtlinie aktivieren, sind in allen Regionen aktiviert, in denen sie verfügbar sind. Um die Ergebnisse für diese Steuerelemente auf nur eine Region zu beschränken, können Sie Ihre AWS Config Rekordereinstellungen aktualisieren und die globale Ressourcenaufzeichnung in allen Regionen außer der Heimatregion deaktivieren. Wenn Sie die zentrale Konfiguration verwenden, fehlt Ihnen die Abdeckung für ein Steuerelement, das in der Heimatregion und einer der verknüpften Regionen nicht verfügbar ist. Eine Liste der Steuerelemente, die globale Ressourcen betreffen, finden Sie unterKontrollen, die sich mit globalen Ressourcen befassen.

Empfohlene Konfigurationsrichtlinie

Wenn Sie zum ersten Mal eine Konfigurationsrichtlinie in der Security Hub-Konsole erstellen, haben Sie die Möglichkeit, die von Security Hub empfohlene Richtlinie auszuwählen.

Die empfohlene Richtlinie aktiviert Security Hub, den Standard AWS Foundational Security Best Practices (FSBP) und alle vorhandenen und neuen FSBP-Steuerelemente. Steuerelemente, die Parameter akzeptieren, verwenden die Standardwerte. Die empfohlene Richtlinie gilt für Root-Benutzer (alle Konten und Organisationseinheiten, sowohl neue als auch bestehende). Nachdem Sie die empfohlene Richtlinie für Ihre Organisation erstellt haben, können Sie sie über das delegierte Administratorkonto ändern. Sie können beispielsweise zusätzliche Standards oder Kontrollen aktivieren oder bestimmte FSBP-Steuerelemente deaktivieren. Anweisungen zum Ändern einer Konfigurationsrichtlinie finden Sie unterAktualisierung der Security Hub Hub-Konfigurationsrichtlinien.

Benutzerdefinierte Konfigurationsrichtlinie

Anstelle der empfohlenen Richtlinie kann der delegierte Administrator bis zu 20 benutzerdefinierte Konfigurationsrichtlinien erstellen. Sie können Ihrer gesamten Organisation eine einzelne benutzerdefinierte Richtlinie oder verschiedene benutzerdefinierte Richtlinien verschiedenen Konten

und Organisationseinheiten zuordnen. Für eine benutzerdefinierte Konfigurationsrichtlinie geben Sie Ihre gewünschten Einstellungen an. Sie können beispielsweise eine benutzerdefinierte Richtlinie erstellen, die FSBP, den Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 und alle Kontrollen in diesen Standards außer Amazon Redshift Redshift-Steuerelementen aktiviert. Die Granularität, die Sie in benutzerdefinierten Konfigurationsrichtlinien verwenden, hängt vom beabsichtigten Umfang der Sicherheitsabdeckung in Ihrem Unternehmen ab.

> **Note**
>
> Sie können dem delegierten Administratorkonto keine Konfigurationsrichtlinie zuordnen, die Security Hub deaktiviert. Eine solche Richtlinie kann mit anderen Konten verknüpft werden, überspringt jedoch die Zuordnung zum delegierten Administrator. Das delegierte Administratorkonto behält seine aktuelle Konfiguration bei.

Nachdem Sie eine benutzerdefinierte Konfigurationsrichtlinie erstellt haben, können Sie zur empfohlenen Konfigurationsrichtlinie wechseln, indem Sie Ihre Konfigurationsrichtlinie entsprechend der empfohlenen Konfiguration aktualisieren. Sie sehen jedoch nicht die Möglichkeit, die empfohlene Konfigurationsrichtlinie zu erstellen, in der Security Hub Hub-Konsole, nachdem Ihre erste Richtlinie erstellt wurde.

Richtlinienverknüpfung durch Anwendung und Vererbung

Wenn Sie sich zum ersten Mal für die zentrale Konfiguration entscheiden, hat Ihre Organisation keine Zuordnungen und verhält sich genauso wie vor der Anmeldung. Der delegierte Administrator kann dann Verknüpfungen zwischen einer Konfigurationsrichtlinie oder einem selbstverwalteten Verhalten und Konten, Organisationseinheiten oder dem Stamm herstellen. Verknüpfungen können durch Anwendung oder Vererbung hergestellt werden.

Über das delegierte Administratorkonto können Sie eine Konfigurationsrichtlinie direkt auf ein Konto, eine Organisationseinheit oder das Stammkonto anwenden. Alternativ kann der delegierte Administrator einem Konto, einer Organisationseinheit oder dem Stammkonto direkt eine selbstverwaltete Bezeichnung zuweisen.

In Ermangelung einer direkten Anwendung erbt ein Konto oder eine Organisationseinheit die Einstellungen der nächstgelegenen übergeordneten Organisation, die über eine Konfigurationsrichtlinie oder ein selbstverwaltetes Verhalten verfügt. Wenn das engste Elternteil mit einer Konfigurationsrichtlinie verknüpft ist, erbt das Kind diese Richtlinie und kann nur vom delegierten Administrator aus der Heimatregion konfiguriert werden. Wenn der nächstgelegene

Elternteil selbst verwaltet wird, erbt das Kind das selbstverwaltete Verhalten und kann in jedem Fall seine eigenen Einstellungen angeben. AWS-Region

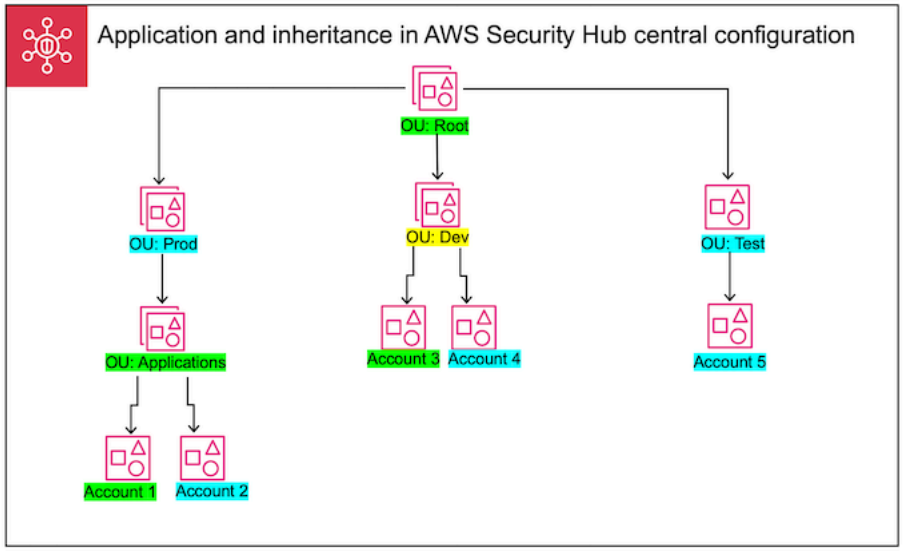
Die Anwendung hat Vorrang vor der Vererbung. Mit anderen Worten, die Vererbung setzt eine Konfigurationsrichtlinie oder eine selbstverwaltete Bestimmung, die der delegierte Administrator direkt auf ein Konto oder eine Organisationseinheit angewendet hat, nicht außer Kraft.

Wenn Sie eine Konfigurationsrichtlinie direkt auf ein selbstverwaltetes Konto anwenden, hat die Richtlinie Vorrang vor der Bezeichnung für selbstverwaltete Konten. Das Konto wird zentral verwaltet und übernimmt die Einstellungen, die in der Konfigurationsrichtlinie enthalten sind.

Wir empfehlen, eine Konfigurationsrichtlinie direkt auf das Stammverzeichnis anzuwenden. Wenn Sie eine Richtlinie auf das Stammverzeichnis anwenden, erben neue Konten, die Ihrer Organisation beitreten, automatisch die Stammrichtlinie, sofern Sie sie nicht einer anderen Richtlinie zuordnen oder sie als selbstverwaltet kennzeichnen.

Einem Konto oder einer Organisationseinheit kann jeweils nur eine Konfigurationsrichtlinie zugeordnet werden, entweder durch Anwendung oder Vererbung. Dadurch sollen widersprüchliche Einstellungen vermieden werden.

Das folgende Diagramm zeigt, wie die Anwendung und Vererbung von Richtlinien in einer zentralen Konfiguration funktionieren.



In diesem Beispiel wurde auf einen grün hervorgehobenen Knoten eine Konfigurationsrichtlinie angewendet. Auf einen blau hervorgehobenen Knoten wurde keine Konfigurationsrichtlinie angewendet. Ein gelb hervorgehobener Knoten wurde als selbstverwaltet eingestuft. Jedes Konto und jede Organisationseinheit verwendet die folgende Konfiguration:

- OU:Root (Grün) — Diese Organisationseinheit verwendet die Konfigurationsrichtlinie, die auf sie angewendet wurde.
- ou:Prod (Blue) — Diese OU erbt die Konfigurationsrichtlinie von OU:Root.
- ou:Applications (Green) — Diese Organisationseinheit verwendet die Konfigurationsrichtlinie, die auf sie angewendet wurde.
- Konto 1 (Grün) — Dieses Konto verwendet die Konfigurationsrichtlinie, die darauf angewendet wurde.
- Konto 2 (Blau) — Dieses Konto erbt die Konfigurationsrichtlinie von OU:Applications.
- ou:Dev (Gelb) — Diese Organisationseinheit wird selbst verwaltet.
- Konto 3 (Grün) — Dieses Konto verwendet die Konfigurationsrichtlinie, die darauf angewendet wurde.
- Konto 4 (Blau) — Dieses Konto erbt das selbstverwaltete Verhalten von OU:Dev.
- ou:Test (Blue) — Dieses Konto erbt die Konfigurationsrichtlinie von ou:Root.
- Konto 5 (Blau) — Dieses Konto erbt die Konfigurationsrichtlinie von ou:Root, da das unmittelbar übergeordnete Konto, ou:Test, keiner Konfigurationsrichtlinie zugeordnet ist.

Testen einer Konfigurationsrichtlinie

Um die Wirkung einer Konfigurationsrichtlinie zu testen, können Sie sie einem einzelnen Konto oder einer einzelnen Organisationseinheit zuordnen, bevor Sie sie in Ihrem gesamten Unternehmen stärker zuordnen.

Um eine Konfigurationsrichtlinie zu testen

1. Erstellen Sie eine benutzerdefinierte Konfigurationsrichtlinie, wenden Sie sie jedoch nicht auf Konten an. Stellen Sie sicher, dass die angegebenen Einstellungen für die Aktivierung, Standards und Kontrollen von Security Hub korrekt sind.
2. Wenden Sie die Konfigurationsrichtlinie auf ein Testkonto oder eine Organisationseinheit an, die keine untergeordneten Konten oder Organisationseinheiten hat.
3. Stellen Sie sicher, dass das Testkonto oder die Organisationseinheit die Konfigurationsrichtlinie in Ihrer Heimatregion und allen verknüpften Regionen erwartungsgemäß verwendet. Sie können auch überprüfen, ob alle anderen Konten und Organisationseinheiten in Ihrer Organisation weiterhin selbst verwaltet werden und dass sie in jeder Region ihre eigenen Einstellungen ändern können.

Nachdem Sie eine Konfigurationsrichtlinie in einem einzelnen Konto oder einer Organisationseinheit getestet haben, können Sie sie mit anderen Konten und Organisationseinheiten verknüpfen. Anweisungen zur Erstellung und Zuordnung von Richtlinien finden Sie unterSecurity Hub Hub-Konfigurationsrichtlinien erstellen und zuordnen. Die untergeordneten Konten der angewendeten Konten erben die Richtlinie, sofern sie nicht selbst verwaltet werden oder für sie eine andere Konfigurationsrichtlinie gilt. Sie können auch Ihre Konfigurationsrichtlinien bearbeiten und bei Bedarf zusätzliche Konfigurationsrichtlinien erstellen.

Security Hub Hub-Konfigurationsrichtlinien erstellen und zuordnen

Das delegierte Administratorkonto kann AWS Security Hub Konfigurationsrichtlinien erstellen und diese mit Organisationskonten, Organisationseinheiten (OUs) oder dem Stamm verknüpfen. Sie können Konten, Organisationseinheiten oder dem Stammverzeichnis auch eine selbstverwaltete Konfiguration zuordnen.

Wenn Sie zum ersten Mal eine Konfigurationsrichtlinie erstellen, empfehlen wir, diese zuerst zu überprüfenSo funktionieren die Security Hub Hub-Konfigurationsrichtlinien.

Wählen Sie Ihre bevorzugte Zugriffsmethode und folgen Sie den Schritten zum Erstellen und Zuordnen einer Konfigurationsrichtlinie oder einer selbstverwalteten Konfiguration. Wenn Sie die Security Hub Hub-Konsole verwenden, können Sie eine Konfiguration mehreren Konten oder Organisationseinheiten gleichzeitig zuordnen. Wenn Sie die Security Hub Hub-API oder verwenden AWS CLI, können Sie eine Konfiguration in jeder Anfrage nur einem Konto oder einer Organisationseinheit zuordnen.

> **Note**
>
> Wenn Sie die zentrale Konfiguration verwenden, deaktiviert Security Hub automatisch Steuerungen, die globale Ressourcen in allen Regionen außer der Heimatregion betreffen. Andere Steuerelemente, die Sie über eine Konfigurationsrichtlinie aktivieren, sind in allen Regionen aktiviert, in denen sie verfügbar sind. Um die Ergebnisse für diese Steuerelemente auf nur eine Region zu beschränken, können Sie Ihre AWS Config Rekordereinstellungen aktualisieren und die globale Ressourcenaufzeichnung in allen Regionen außer der Heimatregion deaktivieren. Wenn Sie die zentrale Konfiguration verwenden, fehlt Ihnen die Abdeckung für ein Steuerelement, das in der Heimatregion und einer der verknüpften Regionen nicht verfügbar ist. Eine Liste der Steuerelemente, die globale Ressourcen betreffen, finden Sie unterKontrollen, die sich mit globalen Ressourcen befassen.

Security Hub console

So erstellen Sie Konfigurationsrichtlinien und ordnen sie zu

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub-Administratorkontos in der Heimatregion an.

2. Wählen Sie im Navigationsbereich Konfiguration und dann die Registerkarte Richtlinien aus. Wählen Sie dann Richtlinie erstellen aus.

3. Wenn Sie zum ersten Mal eine Konfigurationsrichtlinie erstellen, werden auf der Seite Organisation konfigurieren unter Konfigurationstyp drei Optionen angezeigt. Wenn Sie bereits mindestens eine Konfigurationsrichtlinie erstellt haben, wird nur die Option Benutzerdefinierte Richtlinie angezeigt.

   - Wählen Sie Die AWS empfohlene Security Hub Hub-Konfiguration in meiner gesamten Organisation verwenden, um unsere empfohlene Richtlinie zu verwenden. Die empfohlene Richtlinie aktiviert Security Hub in allen Unternehmenskonten, aktiviert den Standard AWS Foundational Security Best Practices (FSBP) und aktiviert alle neuen und vorhandenen FSBP-Steuerelemente. Die Steuerelemente verwenden Standardparameterwerte.
   - Wählen Sie Ich bin noch nicht bereit zur Konfiguration, um später eine Konfigurationsrichtlinie zu erstellen.
   - Wählen Sie Benutzerdefinierte Richtlinie, um eine benutzerdefinierte Konfigurationsrichtlinie zu erstellen. Geben Sie an, ob Security Hub aktiviert oder deaktiviert werden soll, welche Standards aktiviert werden sollen und welche Kontrollen für diese Standards aktiviert werden sollen. Geben Sie optional benutzerdefinierte Parameterwerte für ein oder mehrere aktivierte Steuerelemente an, die benutzerdefinierte Parameter unterstützen.

4. Wählen Sie im Abschnitt Konten aus, für welche Zielkonten, Organisationseinheiten oder das Stammkonto Ihre Konfigurationsrichtlinie gelten soll.

   - Wählen Sie Alle Konten aus, wenn Sie die Konfigurationsrichtlinie auf das Stammkonto anwenden möchten. Dies schließt alle Konten und Organisationseinheiten in der Organisation ein, auf die keine andere Richtlinie angewendet oder vererbt wurde.
   - Wählen Sie Bestimmte Konten aus, wenn Sie die Konfigurationsrichtlinie auf bestimmte Konten oder Organisationseinheiten anwenden möchten. Geben Sie die Konto-IDs ein,

oder wählen Sie die Konten und Organisationseinheiten aus der Organisationsstruktur aus. Sie können die Richtlinie auf maximal 15 Konten oder auf eine Organisationseinheit mit maximal 15 Konten anwenden. Wenn Sie eine größere Anzahl angeben möchten, bearbeiten Sie Ihre Richtlinie nach der Erstellung und wenden Sie sie auf weitere Konten an.

- Wählen Sie Nur der delegierte Administrator, um die Konfigurationsrichtlinie auf das aktuelle delegierte Administratorkonto anzuwenden.

5. Wählen Sie Weiter aus.
6. Überprüfen Sie auf der Seite Überprüfen und Anwenden die Details Ihrer Konfigurationsrichtlinie. Wählen Sie dann Richtlinie erstellen und anwenden aus. In Ihrer Heimatregion und den verknüpften Regionen setzt diese Aktion die vorhandenen Konfigurationseinstellungen der Konten außer Kraft, die dieser Konfigurationsrichtlinie zugeordnet sind. Konten können über eine Anwendung oder durch Vererbung von einem übergeordneten Knoten mit der Konfigurationsrichtlinie verknüpft werden. Untergeordnete Konten und Organisationseinheiten der angewendeten Ziele übernehmen automatisch diese Konfigurationsrichtlinie, sofern sie nicht ausdrücklich ausgeschlossen wurden, sie selbst verwaltet werden oder eine andere Konfigurationsrichtlinie verwenden.

Security Hub API

Um Konfigurationsrichtlinien zu erstellen und zuzuordnen

1. Rufen Sie die CreateConfigurationPolicyAPI über das delegierte Security Hub-Administratorkonto in der Heimatregion auf.
2. Geben Sie für `Name` einen eindeutigen Namen für die Konfigurationsrichtlinie ein. Geben Sie optional für `Description` eine Beschreibung der Konfigurationsrichtlinie an.
3. Geben Sie für das `ServiceEnabled` Feld an, ob Security Hub in dieser Konfigurationsrichtlinie aktiviert oder deaktiviert werden soll.
4. Geben Sie für das `EnabledStandardIdentifiers` Feld an, welche Security Hub Hub-Standards Sie in dieser Konfigurationsrichtlinie aktivieren möchten.
5. Geben Sie für das `SecurityControlsConfiguration` Objekt an, welche Steuerelemente Sie in dieser Konfigurationsrichtlinie aktivieren oder deaktivieren möchten. Wählen Sie `EnabledSecurityControlIdentifiers` aus, dass die angegebenen Steuerelemente aktiviert sind. Andere Steuerelemente, die Teil Ihrer aktivierten Standards sind (einschließlich neu veröffentlichter Steuerelemente), sind deaktiviert. Wenn Sie

`DisabledSecurityControlIdentifiers` diese Option wählen, sind die angegebenen Steuerelemente deaktiviert. Andere Steuerelemente, die Teil Ihrer aktivierten Standards sind (einschließlich neu veröffentlichter Steuerelemente), sind aktiviert.

6. Geben Sie optional für das `SecurityControlCustomParameters` Feld aktivierte Steuerelemente an, für die Sie Parameter anpassen möchten. Geben Sie `CUSTOM` das `ValueType` Feld und den benutzerdefinierten Parameterwert für das `Value` Feld an. Der Wert muss dem richtigen Datentyp entsprechen und innerhalb der von Security Hub angegebenen gültigen Bereiche liegen. Nur ausgewählte Steuerelemente unterstützen benutzerdefinierte Parameterwerte. Weitere Informationen finden Sie unter Benutzerdefinierte Steuerungsparameter.
7. Um Ihre Konfigurationsrichtlinie auf Konten oder Organisationseinheiten anzuwenden, rufen Sie die StartConfigurationPolicyAssociationAPI über das delegierte Security Hub-Administratorkonto in der Heimatregion auf.
8. Geben Sie für das `ConfigurationPolicyIdentifier` Feld den Amazon-Ressourcennamen (ARN) oder die Universally Unique Identifier (UUID) der Richtlinie ein. Der ARN und die UUID werden von der `CreateConfigurationPolicy` API zurückgegeben. Bei einer selbstverwalteten Konfiguration entspricht das `ConfigurationPolicyIdentifier` Feld. `SELF_MANAGED_SECURITY_HUB`
9. Geben Sie für das `Target` Feld die Organisationseinheit, das Konto oder die Root-ID an, für die diese Konfigurationsrichtlinie gelten soll. Sie können in jeder API-Anfrage nur ein Ziel angeben. Untergeordnete Konten und Organisationseinheiten des ausgewählten Ziels erben diese Konfigurationsrichtlinie automatisch, sofern sie nicht selbst verwaltet werden oder eine andere Konfigurationsrichtlinie verwenden.

Beispiel für eine API-Anfrage zur Erstellung einer Konfigurationsrichtlinie:

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
```

```
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Beispiel für eine API-Anfrage zum Zuordnen einer Konfigurationsrichtlinie:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}
```

AWS CLI

Um Konfigurationsrichtlinien zu erstellen und zuzuordnen

1. Führen Sie den create-configuration-policyBefehl über das delegierte Security Hub-Administratorkonto in der Heimatregion aus.
2. Geben Sie für `name` einen eindeutigen Namen für die Konfigurationsrichtlinie ein. Geben Sie optional für `description` eine Beschreibung der Konfigurationsrichtlinie an.

3. Geben Sie für das `ServiceEnabled` Feld an, ob Security Hub in dieser Konfigurationsrichtlinie aktiviert oder deaktiviert werden soll.
4. Geben Sie für das `EnabledStandardIdentifiers` Feld an, welche Security Hub Hub-Standards Sie in dieser Konfigurationsrichtlinie aktivieren möchten.
5. Geben Sie für das `SecurityControlsConfiguration` Feld an, welche Steuerelemente Sie in dieser Konfigurationsrichtlinie aktivieren oder deaktivieren möchten. Wählen Sie `EnabledSecurityControlIdentifiers` aus, dass die angegebenen Steuerelemente aktiviert sind. Andere Steuerelemente, die Teil Ihrer aktivierten Standards sind (einschließlich neu veröffentlichter Steuerelemente), sind deaktiviert. Wenn Sie `DisabledSecurityControlIdentifiers` diese Option wählen, sind die angegebenen Steuerelemente deaktiviert. Andere Steuerelemente, die Ihren aktivierten Standards entsprechen (einschließlich neu veröffentlichter Steuerelemente), sind aktiviert.
6. Geben Sie optional für das `SecurityControlCustomParameters` Feld aktivierte Steuerelemente an, für die Sie Parameter anpassen möchten. Geben Sie `CUSTOM` das `ValueType` Feld und den benutzerdefinierten Parameterwert für das `Value` Feld an. Der Wert muss dem richtigen Datentyp entsprechen und innerhalb der von Security Hub angegebenen gültigen Bereiche liegen. Nur ausgewählte Steuerelemente unterstützen benutzerdefinierte Parameterwerte. Weitere Informationen finden Sie unter Benutzerdefinierte Steuerungsparameter.
7. Um Ihre Konfigurationsrichtlinie auf Konten oder Organisationseinheiten anzuwenden, führen Sie den start-configuration-policy-associationBefehl über das delegierte Security Hub-Administratorkonto in der Heimatregion aus.
8. Geben Sie für das `configuration-policy-identifier` Feld den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie ein. Dieser ARN und diese ID werden vom `create-configuration-policy` Befehl zurückgegeben.
9. Geben Sie für das `target` Feld die Organisationseinheit, das Konto oder die Root-ID an, für die diese Konfigurationsrichtlinie gelten soll. Sie können jedes Mal, wenn Sie den Befehl ausführen, nur ein Ziel angeben. Untergeordnete Objekte des ausgewählten Ziels erben diese Konfigurationsrichtlinie automatisch, sofern sie nicht selbst verwaltet werden oder eine andere Konfigurationsrichtlinie verwenden.

Beispielbefehl zum Erstellen einer Konfigurationsrichtlinie:

```
aws securityhub --region us-east-1 create-configuration-policy \
--name "SampleConfigurationPolicy" \
```

```
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}'
```

Beispielbefehl zum Zuordnen einer Konfigurationsrichtlinie:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}'
```

Die `StartConfigurationPolicyAssociation` API gibt ein Feld namens zurück`AssociationStatus`. In diesem Feld erfahren Sie, ob eine Richtlinienverknüpfung noch aussteht oder ob sie erfolgreich oder nicht erfolgreich ist. Es kann bis zu 24 Stunden dauern, bis sich der Status von `PENDING` zu `SUCCESS` oder ändert`FAILURE`. Weitere Informationen zum Zuordnungsstatus finden Sie unterZuordnungsstatus einer Konfiguration.

Security Hub Hub-Konfigurationsrichtlinien anzeigen

Das delegierte Administratorkonto kann die AWS Security Hub Konfigurationsrichtlinien für eine Organisation und deren Details einsehen.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um Ihre Konfigurationsrichtlinien einzusehen.

Console

Um die Konfigurationsrichtlinien einzusehen

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/.

Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub-Administratorkontos in der Heimatregion an.

2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie die Registerkarte Richtlinien, um einen Überblick über Ihre Konfigurationsrichtlinien zu erhalten.
4. Wählen Sie eine Konfigurationsrichtlinie aus und klicken Sie auf Details anzeigen, um weitere Details dazu anzuzeigen.

API

Um Konfigurationsrichtlinien anzuzeigen

Um eine zusammenfassende Liste all Ihrer Konfigurationsrichtlinien anzuzeigen, rufen Sie die `ListConfigurationPolicies`API über das delegierte Security Hub-Administratorkonto in Ihrer Heimatregion auf. Sie können optionale Paginierungsparameter angeben

Beispiel für eine API-Anfrage:

```
{
    "MaxResults": 5,
    "NextToken": "U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf"
}
```

Um Details zu einer bestimmten Konfigurationsrichtlinie anzuzeigen, rufen Sie die `GetConfigurationPolicy`API über das delegierte Security Hub-Administratorkonto in Ihrer Heimatregion auf. Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie ein, deren Details Sie sehen möchten.

Beispiel für eine API-Anfrage:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Rufen Sie die `ListConfigurationPolicyAssociations`API über das delegierte Administratorkonto von Security Hub in Ihrer Heimatregion auf, um eine zusammenfassende

Liste all Ihrer Konfigurationsrichtlinien und ihrer Verknüpfungen anzuzeigen. Optional können Sie Paginierungsparameter angeben oder die Ergebnisse nach einer bestimmten Richtlinien-ID, einem Zuordnungstyp oder einem Zuordnungsstatus filtern.

Beispiel für eine API-Anfrage:

```
{
    "AssociationType": "APPLIED"
}
```

Um Zuordnungen für ein bestimmtes Konto, eine bestimmte Organisationseinheit oder das Stammkonto anzuzeigen, rufen Sie die BatchGetConfigurationPolicyAssociationsAPI GetConfigurationPolicyAssociationoder über das delegierte Security Hub-Administratorkonto in Ihrer Heimatregion auf. Geben Sie für `Target` die Kontonummer, OU-ID oder Root-ID an.

```
{
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Um Konfigurationsrichtlinien anzuzeigen

Um eine zusammenfassende Liste all Ihrer Konfigurationsrichtlinien anzuzeigen, führen Sie den list-configuration-policiesBefehl über das delegierte Security Hub-Administratorkonto in Ihrer Heimatregion aus.

Beispielbefehl:

```
aws securityhub --region us-east-1 list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf
```

Um Details zu einer bestimmten Konfigurationsrichtlinie anzuzeigen, führen Sie den get-configuration-policyBefehl über das delegierte Security Hub-Administratorkonto in Ihrer Heimatregion aus. Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie ein, deren Details Sie sehen möchten.

```
aws securityhub --region us-east-1 get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Um eine zusammenfassende Liste all Ihrer Konfigurationsrichtlinien und ihrer Kontozuordnungen anzuzeigen, führen Sie den `list-configuration-policy-associations`Befehl über das delegierte Security Hub-Administratorkonto in Ihrer Heimatregion aus. Optional können Sie Paginierungsparameter angeben oder die Ergebnisse nach einer bestimmten Richtlinien-ID, einem Zuordnungstyp oder einem Zuordnungsstatus filtern.

```
aws securityhub --region us-east-1 list-configuration-policy-associations \
--association-type "APPLIED"
```

Um Verknüpfungen für ein bestimmtes Konto anzuzeigen, führen Sie den `batch-get-configuration-policy-associations`Befehl `get-configuration-policy-association`oder vom delegierten Security Hub-Administratorkonto in Ihrer Heimatregion aus. Geben Sie für `target` die Kontonummer, OU-ID oder Root-ID an.

```
aws securityhub --region us-east-1 get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

Zuordnungsstatus einer Konfiguration

Die folgenden API-Operationen für die zentrale Konfiguration geben ein Feld mit dem Namen zurück`AssociationStatus`:

- `BatchGetConfigurationPolicyAssociations`
- `GetConfigurationPolicyAssociation`
- `ListConfigurationPolicyAssociations`
- `StartConfigurationPolicyAssociation`

Dieses Feld wird sowohl zurückgegeben, wenn es sich bei der zugrunde liegenden Konfiguration um eine Konfigurationsrichtlinie handelt, als auch wenn es sich um ein selbstverwaltetes Verhalten handelt.

Der Wert von `AssociationStatus` gibt an, ob eine Richtlinienzuweisung noch aussteht oder ob sie erfolgreich oder nicht erfolgreich ist. Es kann bis zu 24 Stunden dauern, bis sich der Status von `PENDING` zu `SUCCESS` oder ändert`FAILURE`. Der Zuordnungsstatus einer übergeordneten Organisationseinheit oder der Stammorganisation hängt vom Status der untergeordneten Organisationseinheiten ab. Wenn der Assoziationsstatus aller Kinder lautet`SUCCESS`, ist der Assoziationsstatus des Elternteils`SUCCESS`. Wenn der Assoziationsstatus eines oder mehrerer Kinder lautet`FAILED`, ist der Assoziationsstatus des Elternteils`FAILED`.

Der Wert von hängt `AssociationStatus` auch von allen Regionen ab. Wenn die Zuordnung in der Heimatregion und allen verknüpften Regionen erfolgreich ist, `AssociationStatus` ist `SUCCESS` der Wert von. Wenn die Zuordnung in einer oder mehreren dieser Regionen fehlschlägt, hat der `AssociationStatus` Wert `FAILED` von.

Das folgende Verhalten wirkt sich auch auf den Wert von aus`AssociationStatus`:

- Handelt es sich bei dem Ziel um eine übergeordnete Organisationseinheit oder um die Stammorganisation, hat sie nur dann den `AssociationStatus` Wert „Ein“ `SUCCESS` oder „`FAILED`nur“, wenn alle untergeordneten Organisationseinheiten den `FAILED` Status „`SUCCESS`Oder“ haben. Wenn sich der Zuordnungsstatus eines untergeordneten Kontos oder einer Organisationseinheit ändert (z. B. wenn eine verknüpfte Region hinzugefügt oder entfernt wird), nachdem Sie das übergeordnete Konto mit einer Konfiguration verknüpft haben, wird durch die Änderung der Zuordnungsstatus der übergeordneten Einheit nicht aktualisiert, es sei denn, Sie rufen die `StartConfigurationPolicyAssociation` API erneut auf.
- Handelt es sich bei dem Ziel um ein Konto, hat es den `AssociationStatus` Wert „Von“ `SUCCESS` oder `FAILED` nur, wenn die Zuordnung ein Ergebnis von `SUCCESS` oder `FAILED` in der Heimatregion und allen verknüpften Regionen hat. Wenn sich der Zuordnungsstatus eines Zielkontos ändert (z. B. wenn eine verknüpfte Region hinzugefügt oder entfernt wird), nachdem Sie es zum ersten Mal mit einer Konfiguration verknüpft haben, wird sein Zuordnungsstatus aktualisiert. Durch die Änderung wird der Zuordnungsstatus des übergeordneten Elements jedoch nicht aktualisiert, es sei denn, Sie rufen die `StartConfigurationPolicyAssociation` API erneut auf.

Wenn Sie eine neue verknüpfte Region hinzufügen, repliziert Security Hub Ihre vorhandenen Verknüpfungen, die sich in einem `PENDING``SUCCESS`, oder `FAILED` Bundesstaat der neuen Region befinden.

Häufige Gründe für Verbindungsfehler

Eine Zuordnung von Konfigurationsrichtlinien kann aus den folgenden häufigen Gründen fehlschlagen:

- Das Organisationsverwaltungskonto ist kein Mitglied — Wenn Sie dem Organisationsverwaltungskonto eine Konfigurationsrichtlinie zuordnen möchten, muss Security Hub für dieses Konto bereits aktiviert sein. Dadurch wird das Verwaltungskonto zu einem Mitgliedskonto in der Organisation.
- AWS Configist nicht aktiviert oder nicht richtig konfiguriert — Um Standards in einer Konfigurationsrichtlinie zu aktivieren, AWS Config muss sie aktiviert und konfiguriert sein, um relevante Ressourcen aufzuzeichnen.
- Die Verknüpfung muss über ein delegiertes Administratorkonto erfolgen — Sie können eine Richtlinie nur Zielkonten und Organisationseinheiten zuordnen, wenn Sie mit dem delegierten Administratorkonto angemeldet sind.
- Verbindung muss von der Heimatregion aus erfolgen — Sie können eine Richtlinie nur Zielkonten und Organisationseinheiten zuordnen, wenn Sie in der Heimatregion angemeldet sind.
- Opt-in-Region nicht aktiviert — Die Richtlinienzuweisung schlägt für ein Mitgliedskonto oder eine Organisationseinheit in einer verknüpften Region fehl, wenn es sich um eine Opt-in-Region handelt, die der delegierte Administrator nicht aktiviert hat. Sie können es erneut versuchen, nachdem Sie die Region über das delegierte Administratorkonto aktiviert haben.
- Mitgliedskonto gesperrt — Die Richtlinienverknüpfung schlägt fehl, wenn Sie versuchen, eine Richtlinie mit einem gesperrten Mitgliedskonto zu verknüpfen.

Aktualisierung der Security Hub Hub-Konfigurationsrichtlinien

Das delegierte Administratorkonto kann die AWS Security Hub Konfigurationsrichtlinien nach Bedarf aktualisieren. Der delegierte Administrator kann die Richtlinieneinstellungen, die Konten oder Organisationseinheiten, denen eine Richtlinie zugeordnet ist, oder beides aktualisieren. Wenn die Richtlinieneinstellungen aktualisiert werden, verwenden Konten, die der Konfigurationsrichtlinie zugeordnet sind, automatisch die aktualisierte Richtlinie.

Ähnlich wie bei der Erstellung der Konfigurationsrichtlinie können Sie die folgenden Richtlinieneinstellungen aktualisieren:

- Aktivieren oder deaktivieren Sie Security Hub.

- Aktivieren Sie einen oder mehrere Sicherheitsstandards.
- Geben Sie an, welche Sicherheitskontrollen für alle aktivierten Standards aktiviert sind. Sie können dies tun, indem Sie eine Liste bestimmter Steuerelemente bereitstellen, die aktiviert werden sollten, und Security Hub deaktiviert alle anderen Steuerelemente, einschließlich neuer Steuerelemente, wenn sie veröffentlicht werden. Alternativ können Sie eine Liste mit bestimmten Steuerelementen bereitstellen, die deaktiviert werden sollten, und Security Hub aktiviert alle anderen Kontrollen, einschließlich neuer Steuerelemente, wenn sie veröffentlicht werden.
- Passen Sie optional die Parameter für ausgewählte aktivierte Steuerelemente für alle aktivierten Standards an.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zum Aktualisieren einer Konfigurationsrichtlinie.

Wenn Sie die zentrale Konfiguration verwenden, deaktiviert Security Hub automatisch Steuerungen, die globale Ressourcen in allen Regionen außer der Heimatregion betreffen. Andere Steuerelemente, die Sie über eine Konfigurationsrichtlinie aktivieren, sind in allen Regionen aktiviert, in denen sie verfügbar sind. Um die Ergebnisse für diese Steuerelemente auf nur eine Region zu beschränken, können Sie Ihre AWS Config Rekordereinstellungen aktualisieren und die globale Ressourcenaufzeichnung in allen Regionen außer der Heimatregion deaktivieren. Wenn Sie die zentrale Konfiguration verwenden, fehlt Ihnen die Abdeckung für ein Steuerelement, das in der Heimatregion und einer der verknüpften Regionen nicht verfügbar ist. Eine Liste der Steuerelemente, die globale Ressourcen betreffen, finden Sie unterKontrollen, die sich mit globalen Ressourcen befassen.

Console

So aktualisieren Sie die Konfigurationsrichtlinien

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub-Administratorkontos in der Heimatregion an.
2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie die Registerkarte Policies.
4. Wählen Sie die Konfigurationsrichtlinie aus, die Sie bearbeiten möchten, und wählen Sie Bearbeiten aus. Falls gewünscht, bearbeiten Sie die Richtlinieneinstellungen. Lassen Sie

diesen Abschnitt unverändert, wenn Sie die Richtlinieneinstellungen unverändert lassen möchten.

5. Wählen Sie Weiter. Falls gewünscht, bearbeiten Sie die Richtlinienverknüpfungen. Lassen Sie diesen Abschnitt unverändert, wenn Sie die Richtlinienverknüpfungen unverändert lassen möchten.
6. Wählen Sie Weiter aus.
7. Überprüfen Sie Ihre Änderungen und wählen Sie Speichern und anwenden. In Ihrer Heimatregion und den verknüpften Regionen setzt diese Aktion die vorhandenen Konfigurationseinstellungen der Konten außer Kraft, die dieser Konfigurationsrichtlinie zugeordnet sind. Konten können über eine Anwendung oder durch Vererbung von einem übergeordneten Knoten mit einer Konfigurationsrichtlinie verknüpft werden.

API

Um die Konfigurationsrichtlinien zu aktualisieren

1. Um die Einstellungen in einer Konfigurationsrichtlinie zu aktualisieren, rufen Sie die UpdateConfigurationPolicyAPI über das delegierte Security Hub-Administratorkonto in der Heimatregion auf.
2. Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, die Sie aktualisieren möchten.
3. Geben Sie aktualisierte Werte für die Felder unter ein`ConfigurationPolicy`. Optional können Sie auch einen Grund für die Aktualisierung angeben.
4. Um neue Verknüpfungen für diese Konfigurationsrichtlinie hinzuzufügen, rufen Sie die StartConfigurationPolicyAssociationAPI über das delegierte Security Hub-Administratorkonto in der Heimatregion auf. Um eine oder mehrere aktuelle Verknüpfungen zu entfernen, rufen Sie die StartConfigurationPolicyDisassociationAPI über das delegierte Security Hub-Administratorkonto in der Heimatregion auf.
5. Geben Sie für das `ConfigurationPolicyIdentifier` Feld den ARN oder die ID der Konfigurationsrichtlinie ein, deren Verknüpfungen Sie aktualisieren möchten.
6. Geben Sie für das `Target` Feld die Konten, Organisationseinheiten oder die Root-ID ein, die Sie zuordnen oder trennen möchten. Diese Aktion setzt vorherige Richtlinienzuordnungen für die angegebenen Organisationseinheiten oder Konten außer Kraft.

> **Note**
>
> Wenn Sie die `UpdateConfigurationPolicy` API aufrufen, führt Security Hub eine vollständige Listenersetzung für die `SecurityControlCustomParameters` Felder`EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiers``DisabledSecurityControlIdentifiers`, und durch. Geben Sie bei jedem Aufruf dieser API die vollständige Liste der Standards an, die Sie aktivieren möchten, sowie die vollständige Liste der Steuerelemente, die Sie aktivieren oder deaktivieren und für die Sie die Parameter anpassen möchten.

Beispiel für eine API-Anfrage zur Aktualisierung einer Konfigurationsrichtlinie:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Disabling CloudWatch.1",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2",
                    "CloudWatch.1"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
```

```
                        }
                    }
                ]
            }
        }
    }
}
```

AWS CLI

Um die Konfigurationsrichtlinien zu aktualisieren

1. Um die Einstellungen in einer Konfigurationsrichtlinie zu aktualisieren, führen Sie den update-configuration-policyBefehl über das delegierte Security Hub-Administratorkonto in der Heimatregion aus.
2. Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, die Sie aktualisieren möchten.
3. Geben Sie aktualisierte Werte für die Felder unter ein`configuration-policy`. Optional können Sie auch einen Grund für die Aktualisierung angeben.
4. Um neue Verknüpfungen für diese Konfigurationsrichtlinie hinzuzufügen, führen Sie den start-configuration-policy-associationBefehl über das delegierte Security Hub-Administratorkonto in der Heimatregion aus. Um eine oder mehrere aktuelle Verknüpfungen zu entfernen, führen Sie den start-configuration-policy-disassociationBefehl über das delegierte Security Hub-Administratorkonto in der Heimatregion aus.
5. Geben Sie für das `configuration-policy-identifier` Feld den ARN oder die ID der Konfigurationsrichtlinie ein, deren Verknüpfungen Sie aktualisieren möchten.
6. Geben Sie für das `target` Feld die Konten, Organisationseinheiten oder die Root-ID ein, die Sie zuordnen oder trennen möchten. Diese Aktion setzt vorherige Richtlinienzuordnungen für die angegebenen Organisationseinheiten oder Konten außer Kraft.

> **Note**
>
> Wenn Sie den `update-configuration-policy` Befehl ausführen, führt Security Hub eine vollständige Listenersetzung für die `SecurityControlCustomParameters` Felder `EnabledStandardIdentifiersEnabledSecurityControlIdentifiers`,`DisabledSecuri` und durch. Geben Sie bei jeder Ausführung dieses Befehls die vollständige Liste

der Standards an, die Sie aktivieren möchten, sowie die vollständige Liste der Steuerelemente, die Sie aktivieren oder deaktivieren und deren Parameter anpassen möchten.

Beispielbefehl zum Aktualisieren einer Konfigurationsrichtlinie:

```
aws securityhub update-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--description "Updated configuration policy" \
--updated-reason "Disabling CloudWatch.1" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2","CloudWatch.1"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}}'
```

Die `StartConfigurationPolicyAssociation` API gibt ein Feld namens zurück`AssociationStatus`. In diesem Feld erfahren Sie, ob eine Richtlinienverknüpfung noch aussteht oder ob sie erfolgreich oder nicht erfolgreich ist. Es kann bis zu 24 Stunden dauern, bis sich der Status von `PENDING` zu `SUCCESS` oder ändert`FAILURE`. Weitere Informationen zum Zuordnungsstatus finden Sie unterZuordnungsstatus einer Konfiguration.

Security Hub Hub-Konfigurationsrichtlinien löschen und deren Zuordnung aufheben

Das delegierte Administratorkonto kann eine AWS Security Hub Konfigurationsrichtlinie löschen. Alternativ kann das delegierte Administratorkonto die Konfigurationsrichtlinie beibehalten, sie jedoch von bestimmten Konten oder Organisationseinheiten (OUs) trennen.

Im folgenden Abschnitt werden diese beiden Optionen erläutert.

Löschen von Konfigurationsrichtlinien

Wenn Sie eine Konfigurationsrichtlinie löschen, ist sie für Ihr Unternehmen nicht mehr vorhanden. Zielkonten, Organisationseinheiten und das Stammverzeichnis der Organisation können die Konfigurationsrichtlinie nicht mehr verwenden. Ziele, die mit einer gelöschten Konfigurationsrichtlinie verknüpft waren, erben die Konfigurationsrichtlinie des nächstgelegenen übergeordneten Objekts oder werden selbst verwaltet, wenn das nächstgelegene übergeordnete Objekt selbst verwaltet wird. Wenn Sie möchten, dass ein Ziel eine andere Konfiguration verwendet, können Sie das Ziel einer neuen Konfigurationsrichtlinie zuordnen. Weitere Informationen finden Sie unter Security Hub Hub-Konfigurationsrichtlinien erstellen und zuordnen.

Wir empfehlen, mindestens eine Konfigurationsrichtlinie zu erstellen und mit Ihrer Organisation zu verknüpfen, um einen angemessenen Sicherheitsschutz zu gewährleisten.

Bevor Sie eine Konfigurationsrichtlinie löschen können, müssen Sie die Zuordnung der Richtlinie zu Konten, Organisationseinheiten oder dem Stammverzeichnis aufheben, für das sie derzeit gilt.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zum Löschen einer Konfigurationsrichtlinie.

Console

Um eine Konfigurationsrichtlinie zu löschen

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub-Administratorkontos in der Heimatregion an.
2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie die Registerkarte Policies. Wählen Sie die Konfigurationsrichtlinie aus, die Sie löschen möchten, und wählen Sie Löschen aus. Wenn die Konfigurationsrichtlinie noch mit Konten oder Organisationseinheiten verknüpft ist, werden Sie aufgefordert, die Richtlinie zunächst von diesen Zielen zu trennen, bevor Sie sie löschen können.
4. Überprüfen Sie die Bestätigungsnachricht. Geben Sie ein **`confirm`** und wählen Sie Löschen.

API

Um eine Konfigurationsrichtlinie zu löschen

Rufen Sie die DeleteConfigurationPolicyAPI über das delegierte Security Hub-Administratorkonto in der Heimatregion auf.

Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, die Sie löschen möchten. Wenn Sie eine `ConflictException` Fehlermeldung erhalten, gilt die Konfigurationsrichtlinie weiterhin für Konten oder Organisationseinheiten in Ihrer Organisation. Um den Fehler zu beheben, trennen Sie die Konfigurationsrichtlinie von diesen Konten oder Organisationseinheiten, bevor Sie versuchen, sie zu löschen.

Beispiel für eine API-Anfrage zum Löschen einer Konfigurationsrichtlinie:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

Um eine Konfigurationsrichtlinie zu löschen

Führen Sie den delete-configuration-policyBefehl über das delegierte Security Hub-Administratorkonto in der Heimatregion aus.

Geben Sie den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, die Sie löschen möchten. Wenn Sie eine `ConflictException` Fehlermeldung erhalten, gilt die Konfigurationsrichtlinie weiterhin für Konten oder Organisationseinheiten in Ihrer Organisation. Um den Fehler zu beheben, trennen Sie die Konfigurationsrichtlinie von diesen Konten oder Organisationseinheiten, bevor Sie versuchen, sie zu löschen.

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Aufheben der Zuordnung einer Konfiguration zu Konten und Organisationseinheiten

Mit dem delegierten Administratorkonto können Sie die Zuordnung eines Zielkontos, einer Organisationseinheit oder eines Stammkontos zu einer aktuell geltenden Konfigurationsrichtlinie

oder zu einer selbstverwalteten Konfiguration aufheben. Sie können die Zuordnung eines Ziels nur zu einer angewendeten Konfiguration aufheben, nicht zu einer geerbten Konfiguration. Um eine geerbte Konfiguration zu ändern, können Sie eine Konfigurationsrichtlinie oder ein selbstverwaltetes Verhalten auf das betroffene Konto oder die betroffene Organisationseinheit anwenden. Sie können auch eine neue Konfigurationsrichtlinie, die Ihre gewünschten Änderungen enthält, auf das nächstgelegene übergeordnete Objekt anwenden.

Durch die Trennung der Zuordnung wird eine Konfigurationsrichtlinie nicht gelöscht. Die Richtlinie wird in Ihrem Konto gespeichert, sodass Sie sie mit anderen Zielen in Ihrer Organisation verknüpfen können. Wenn die Trennung abgeschlossen ist, erbt ein betroffenes Ziel die Konfigurationsrichtlinie oder das selbstverwaltete Verhalten des nächstgelegenen übergeordneten Ziels. Wenn es keine vererbbare Konfiguration gibt, behält ein Ziel die Einstellungen bei, die es vor der Trennung hatte, wird aber selbst verwaltet.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um ein Konto, eine Organisationseinheit oder einen Root-Benutzer von der aktuellen Konfiguration zu trennen.

Console

Um ein Konto oder eine Organisationseinheit von der aktuellen Konfiguration zu trennen

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub-Administratorkontos in der Heimatregion an.
2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie auf der Registerkarte Organizations das Konto, die Organisationseinheit oder das Stammverzeichnis aus, das Sie von der aktuellen Konfiguration trennen möchten. Wählen Sie Bearbeiten aus.
4. Wählen Sie auf der Seite Konfiguration definieren für Verwaltung die Option Anwendete Richtlinie aus, wenn der delegierte Administrator Richtlinien direkt auf das Ziel anwenden kann. Wählen Sie Vererbt aus, wenn das Ziel die Konfiguration seines nächstgelegenen übergeordneten Objekts erben soll. In beiden Fällen kontrolliert der delegierte Administrator die Einstellungen für das Ziel. Wählen Sie Selbstverwaltet, wenn Sie möchten, dass das Konto oder die Organisationseinheit ihre eigenen Einstellungen steuert.
5. Nachdem Sie Ihre Änderungen überprüft haben, wählen Sie Weiter und Anwenden. Diese Aktion setzt bestehende Konfigurationen aller Konten oder Organisationseinheiten außer

Kraft, die im Gültigkeitsbereich enthalten sind, falls diese Konfigurationen mit Ihrer aktuellen Auswahl in Konflikt stehen.

API

Um ein Konto oder eine Organisationseinheit von der aktuellen Konfiguration zu trennen

1. Rufen Sie die StartConfigurationPolicyDisassociationAPI über das delegierte Security Hub-Administratorkonto in der Heimatregion auf.
2. Geben Sie für `ConfigurationPolicyIdentifier` den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, deren Zuordnung Sie aufheben möchten. Geben Sie dieses Feld an, `SELF_MANAGED_SECURITY_HUB` um die Zuordnung zu selbstverwaltetem Verhalten aufzuheben.
3. Geben Sie für `Target` die Konten, Organisationseinheiten oder den Stamm an, die Sie von dieser Konfigurationsrichtlinie trennen möchten.

Beispiel für eine API-Anfrage zum Trennen der Zuordnung zu einer Konfigurationsrichtlinie:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

Um ein Konto oder eine Organisationseinheit von der aktuellen Konfiguration zu trennen

1. Führen Sie den start-configuration-policy-disassociationBefehl über das delegierte Security Hub-Administratorkonto in der Heimatregion aus.
2. Geben Sie für `configuration-policy-identifier` den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie an, deren Zuordnung Sie aufheben möchten. Geben Sie dieses Feld an, `SELF_MANAGED_SECURITY_HUB` um die Zuordnung zu selbstverwaltetem Verhalten aufzuheben.
3. Geben Sie für `target` die Konten, Organisationseinheiten oder den Stamm an, die Sie von dieser Konfigurationsrichtlinie trennen möchten.

Beispielbefehl zum Trennen der Zuordnung einer Konfigurationsrichtlinie:

```
aws securityhub --region us-east-1 start-configuration-policy-disassociation \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"RootId": "r-f6g7h8i9j0example"}'
```

Zentrale Konfiguration im Rahmen eines Standards oder einer Steuerung

Sie können die zentrale Konfiguration auf der Konfigurationsseite der AWS Security Hub Konsole oder im Kontext eines bestimmten Sicherheitsstandards oder einer bestimmten Sicherheitskontrolle verwenden. Wenn Sie diese Funktion im Kontext verwenden, können Sie Standards und Kontrollen in Ihrer gesamten Organisation so konfigurieren, dass sie in bestehende Workflows integriert sind. Wenn Sie sich die Ergebnisse ansehen, können Sie außerdem herausfinden, welche Standards und Kontrollen für Ihre Umgebung am relevantesten sind, und sie gleichzeitig konfigurieren.

Die kontextabhängige Konfiguration ist nur auf der Security Hub Hub-Konsole verfügbar. Programmgesteuert müssen Sie die UpdateConfigurationPolicyAPI aufrufen, um die Konfiguration bestimmter Standards oder Kontrollen in Ihrer Organisation zu ändern.

Einen Sicherheitsstandard im Kontext konfigurieren

Folgen Sie den Schritten, um einen Sicherheitsstandard kontextbezogen über die zentrale Konfiguration zu konfigurieren.

So konfigurieren Sie einen Sicherheitsstandard im Kontext (nur Konsole)

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub-Administratorkontos in der Heimatregion an.
2. Wählen Sie im Navigationsbereich Sicherheitsstandards aus.
3. Wählen Sie für den Standard, den Sie konfigurieren möchten, die Option Konfigurieren aus. Sie können auch einen bestimmten Standard auswählen und dann auf der Standarddetailseite die Option Konfigurieren auswählen. Die Konsole listet Ihre vorhandenen Security Hub Hub-

Konfigurationsrichtlinien (Konfigurationsrichtlinien) und den Status dieses Standards in jeder einzelnen auf.

4. Wählen Sie in jeder Konfigurationsrichtlinie die Optionen aus, um den Standard zu aktivieren oder zu deaktivieren.
5. Nachdem Sie Ihre Änderungen vorgenommen haben, wählen Sie Weiter.
6. Überprüfen Sie Ihre Änderungen und wählen Sie Anwenden. Diese Aktion wirkt sich auf alle Konten und Organisationseinheiten aus, die einer Konfigurationsrichtlinie zugeordnet sind. Ihre Konfiguration wird in der Heimatregion und allen verknüpften Regionen wirksam.

Konfiguration einer Sicherheitskontrolle im Kontext

Folgen Sie den Schritten zur kontextbezogenen Konfiguration einer Sicherheitskontrolle über die zentrale Konfiguration.

So konfigurieren Sie eine Sicherheitskontrolle im Kontext (nur Konsole)

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub-Administratorkontos in der Heimatregion an.
2. Wählen Sie im Navigationsbereich Controls aus.
3. Wählen Sie ein bestimmtes Steuerelement und dann Konfigurieren aus. In der Konsole werden Ihre aktuellen Konfigurationsrichtlinien und der Status dieser Steuerung in den einzelnen Richtlinien aufgeführt.
4. Wählen Sie in jeder Konfigurationsrichtlinie die Optionen aus, um die Steuerung zu aktivieren oder zu deaktivieren. Sie können sich auch dafür entscheiden, die Steuerungsparameter anzupassen.
5. Nachdem Sie Ihre Änderungen vorgenommen haben, wählen Sie Weiter.
6. Überprüfen Sie Ihre Änderungen und wählen Sie Anwenden. Diese Aktion wirkt sich auf alle Konten und Organisationseinheiten aus, die einer Konfigurationsrichtlinie zugeordnet sind. Ihre Konfiguration wird in der Heimatregion und allen verknüpften Regionen wirksam.

Beenden Sie die Verwendung der zentralen Konfiguration

Wenn Sie die zentrale Konfiguration in nicht mehr verwendenAWS Security Hub, verliert der delegierte Administrator die Möglichkeit, Security Hub, Sicherheitsstandards und Sicherheitskontrollen für mehrere AWS-Konten Organisationseinheiten (OUs) zu konfigurieren, undAWS-Regionen. Stattdessen müssen Unternehmenskonten die meisten ihrer eigenen Einstellungen in jeder Region separat konfigurieren.

> **Important**
>
> Bevor Sie die zentrale Konfiguration nicht mehr verwenden können, müssen Sie zunächst Ihre Konten und Organisationseinheiten von ihrer aktuellen Konfiguration trennen, unabhängig davon, ob es sich dabei um eine Konfigurationsrichtlinie oder ein selbstverwaltetes Verhalten handelt.
> Bevor Sie die zentrale Konfiguration nicht mehr verwenden können, müssen Sie auch Ihre Konfigurationsrichtlinien löschen.

Wenn Sie die zentrale Konfiguration beenden, treten die folgenden Änderungen auf:

- Der delegierte Administrator kann keine Konfigurationsrichtlinien mehr für die Organisation erstellen.
- Konten, auf die eine Konfigurationsrichtlinie angewendet oder vererbt wurde, behalten ihre aktuellen Einstellungen bei, werden jedoch automatisch verwaltet.
- Ihr Unternehmen wechselt zur lokalen Konfiguration. Bei der lokalen Konfiguration müssen die meisten Security Hub Hub-Einstellungen für jedes Organisationskonto und jede Region separat konfiguriert werden. Der delegierte Administrator kann wählen, ob Security Hub, Standardsicherheitsstandards und alle Kontrollen, die Teil der Standardstandards sind, in neuen Organisationskonten automatisch aktiviert werden. Die Standardstandards sind AWS Foundational Security Best Practices (FSBP) und Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Diese Einstellungen sind nur in der aktuellen Region wirksam und wirken sich nur auf neue Unternehmenskonten aus. Der delegierte Administrator kann nicht ändern, welche Standards die Standardstandards sind. Die lokale Konfiguration unterstützt nicht die Verwendung von Konfigurationsrichtlinien oder Konfigurationen auf OU-Ebene.

Die Identität des delegierten Administratorkontos bleibt unverändert, wenn Sie die zentrale Konfiguration nicht mehr verwenden. Ihre Heimatregion und die verknüpften Regionen bleiben

ebenfalls unverändert (Ihre Heimatregion wird jetzt als Aggregationsregion bezeichnet und kann für die Suche nach Aggregationen verwendet werden).

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um die zentrale Konfiguration nicht mehr zu verwenden und zur lokalen Konfiguration zu wechseln.

Security Hub console

Um die zentrale Konfiguration nicht mehr zu verwenden

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub-Administratorkontos in der Heimatregion an.
2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie im Abschnitt Übersicht die Option Bearbeiten aus.
4. Wählen Sie im Feld Organisationskonfiguration bearbeiten die Option Lokale Konfiguration aus. Falls Sie dies noch nicht getan haben, werden Sie aufgefordert, Ihre aktuellen Konfigurationsrichtlinien zu trennen und zu löschen, bevor Sie die zentrale Konfiguration beenden können. Konten oder Organisationseinheiten, die als selbstverwaltet gekennzeichnet sind, müssen von ihrer selbstverwalteten Konfiguration getrennt werden. Sie können dies in der Konsole tun, indem Sie den Verwaltungstyp jedes selbstverwalteten Kontos oder jeder Organisationseinheit auf Zentral verwaltet und von meiner Organisation übernehmen ändern.
5. Wählen Sie optional die Standardeinstellungen für die lokale Konfiguration für neue Organisationskonten aus.
6. Wählen Sie Bestätigen aus.

Security Hub API

Um die zentrale Konfiguration nicht mehr zu verwenden

1. Rufen Sie die UpdateOrganizationConfigurationAPI auf.
2. Setzen Sie das `ConfigurationType` Feld im `OrganizationConfiguration` Objekt auf`LOCAL`. Die API gibt einen Fehler zurück, wenn Sie über bestehende Konfigurationsrichtlinien oder Richtlinienzuordnungen verfügen. Rufen Sie

die API auf, um die Zuordnung einer Konfigurationsrichtlinie aufzuheben. `StartConfigurationPolicyDisassociation` Rufen Sie die API auf, um eine Konfigurationsrichtlinie zu löschen. `DeleteConfigurationPolicy`

3. Wenn Sie Security Hub automatisch in neuen Organisationskonten aktivieren möchten, setzen Sie das `AutoEnable` Feld auf`true`. Standardmäßig ist der Wert dieses Feldes`false`, und Security Hub wird in neuen Organisationskonten nicht automatisch aktiviert. Wenn Sie die Standardsicherheitsstandards für neue Organisationskonten automatisch aktivieren möchten, setzen Sie das `AutoEnableStandards` Feld optional auf`DEFAULT`. Dies ist der Standardwert. Wenn Sie die Standardsicherheitsstandards in neuen Organisationskonten nicht automatisch aktivieren möchten, setzen Sie das `AutoEnableStandards` Feld auf`NONE`.

Beispiel für eine API-Anfrage:

```
{
    "AutoEnable": true,
    "OrganizationConfiguration": {
        "ConfigurationType" : "LOCAL"
    }
}
```

AWS CLI

Um die zentrale Konfiguration nicht mehr zu verwenden

1. Führen Sie den Befehl update-organization-configuration aus.
2. Stellen Sie das `ConfigurationType` Feld im `organization-configuration` Objekt auf ein`LOCAL`. Der Befehl gibt einen Fehler zurück, wenn Sie bereits über Konfigurationsrichtlinien oder Richtlinienzuordnungen verfügen. Führen Sie den `start-configuration-policy-disassociation` Befehl aus, um die Zuordnung einer Konfigurationsrichtlinie aufzuheben. Führen Sie den `delete-configuration-policy` Befehl aus, um eine Konfigurationsrichtlinie zu löschen.
3. Wenn Sie Security Hub automatisch in neuen Organisationskonten aktivieren möchten, geben Sie den `auto-enable` Parameter an. Standardmäßig ist der Wert dieses Parameters`no-auto-enable`, und Security Hub wird in neuen Organisationskonten nicht automatisch aktiviert. Wenn Sie die Standardsicherheitsstandards für neue

Organisationskonten automatisch aktivieren möchten, setzen Sie das `auto-enable-standards` Feld optional auf`DEFAULT`. Dies ist der Standardwert. Wenn Sie die Standardsicherheitsstandards in neuen Organisationskonten nicht automatisch aktivieren möchten, setzen Sie das `auto-enable-standards` Feld auf`NONE`.

```
aws securityhub --region us-east-1 update-organization-configuration \
--auto-enable \
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

Verwaltung von Administrator- und Mitgliedskonten

Wenn Ihre AWS Umgebung über mehrere Konten verfügt, können Sie die Konten, die AWS Security Hub verwenden, als Mitgliedskonten behandeln und sie einem einzigen Administratorkonto zuordnen. Der Administrator kann Ihren allgemeinen Sicherheitsstatus überwachen und zulässige Aktionen für Mitgliedskonten ergreifen. Der Administrator kann auch verschiedene Aufgaben zur Kontoverwaltung und -verwaltung in großem Umfang ausführen, z. B. die Überwachung der geschätzten Nutzungskosten und die Bewertung der Kontokontingente.

Sie können Mitgliedskonten auf zwei Arten mit einem Administrator verknüpfen, indem Sie Security Hub in Security Hub integrieren AWS Organizations oder indem Sie Mitgliedschaftseinladungen manuell in Security Hub senden und annehmen.

Verwalten von Konten mit AWS Organizations

AWS Organizationsist ein globaler Kontoverwaltungsdienst, mit dem AWS Administratoren mehrere Konten konsolidieren und verwalten könnenAWS-Konten. Er bietet Funktionen zur Kontoverwaltung und konsolidierten Fakturierung, die auf die Erfüllung von Haushalts-, Sicherheits- und Compliance-Anforderungen zugeschnitten sind. Es wird ohne zusätzliche Kosten angeboten und lässt sich in mehrere integrierenAWS-Services, darunter AWS Security Hub, Amazon Macie und Amazon GuardDuty. Weitere Informationen finden Sie im AWS Organizations-Benutzerhandbuch.

Wenn Sie Security Hub und integrierenAWS Organizations, bestimmt das Verwaltungskonto der Organizations einen delegierten Security Hub-Administrator. Security Hub wird automatisch in dem delegierten Administratorkonto aktiviert, AWS-Region in dem es zugewiesen wurde.

Nach der Benennung eines delegierten Administrators empfehlen wir, Konten in Security Hub mit zentraler Konfiguration zu verwalten. Dies ist die effizienteste Methode, um Security Hub individuell anzupassen und eine angemessene Sicherheitsabdeckung für Ihr Unternehmen sicherzustellen.

Durch die zentrale Konfiguration kann der delegierte Administrator Security Hub für mehrere Unternehmenskonten und Regionen anpassen, anstatt es von Region zu Region zu konfigurieren. Sie können eine Konfigurationsrichtlinie für Ihr gesamtes Unternehmen oder unterschiedliche Konfigurationsrichtlinien für verschiedene Konten und Organisationseinheiten erstellen. Die Richtlinien geben an, ob Security Hub in den zugehörigen Konten aktiviert oder deaktiviert ist und welche Sicherheitsstandards und Kontrollen aktiviert sind.

Der delegierte Administrator kann Konten als zentral verwaltete oder selbstverwaltete Konten festlegen. Zentral verwaltete Konten können nur vom delegierten Administrator konfiguriert werden. Selbstverwaltete Konten können ihre eigenen Einstellungen angeben.

Wenn Sie sich nicht für die zentrale Konfiguration entscheiden, hat der delegierte Administrator eine eingeschränktere Möglichkeit, Security Hub zu konfigurieren, was als lokale Konfiguration bezeichnet wird. Bei der lokalen Konfiguration kann der delegierte Administrator Security Hub und Standardsicherheitsstandards in neuen Unternehmenskonten in der aktuellen Region automatisch aktivieren. Bestehende Konten verwenden diese Einstellungen jedoch nicht, sodass es nach dem Beitritt eines Kontos zur Organisation zu Konfigurationsabweichungen kommen kann.

Abgesehen von diesen neuen Kontoeinstellungen ist die lokale Konfiguration konto- und regionsspezifisch. Jedes Organisationskonto muss den Security Hub Hub-Dienst, die Standards und die Kontrollen in jeder Region separat konfigurieren. Die lokale Konfiguration unterstützt auch nicht die Verwendung von Konfigurationsrichtlinien.

Manuelles Verwalten von Konten auf Einladung

Sie müssen Mitgliedskonten auf Einladung manuell in Security Hub verwalten, wenn Sie ein eigenständiges Konto haben oder wenn Sie nicht in Organizations integriert sind. Ein eigenständiges Konto kann nicht in Organizations integriert werden, daher muss es manuell verwaltet werden. Wir empfehlen, die zentrale Konfiguration zu integrieren AWS Organizations und diese zu verwenden, wenn Sie in future weitere Konten hinzufügen.

Wenn Sie die manuelle Kontoverwaltung verwenden, bestimmen Sie ein Konto als Security Hub-Administrator. Das Administratorkonto kann Daten in Mitgliedskonten einsehen und anhand der Ergebnisse von Mitgliedskonten bestimmte Maßnahmen ergreifen. Der Security Hub-Administrator lädt andere Konten als Mitgliedskonten ein, und die Beziehung zwischen Administrator und Mitglied wird hergestellt, wenn ein potenzielles Mitgliedskonto die Einladung annimmt.

Die manuelle Kontoverwaltung unterstützt die Verwendung von Konfigurationsrichtlinien nicht. Ohne Konfigurationsrichtlinien kann der Administrator Security Hub nicht zentral anpassen, indem er variable Einstellungen für verschiedene Konten konfiguriert. Stattdessen muss jedes Organisationskonto Security Hub für sich selbst in jeder Region separat aktivieren und konfigurieren. Dies kann es schwieriger und zeitaufwändiger machen, eine angemessene Sicherheitsabdeckung für alle Konten und Regionen sicherzustellen, in denen Sie Security Hub verwenden. Dies kann auch zu Konfigurationsabweichungen führen, da Mitgliedskonten ihre eigenen Einstellungen ohne Eingaben des Administrators angeben können.

Informationen zur Verwaltung von Konten auf Einladung finden Sie unterVerwalten von Konten auf Einladung.

Konten verwalten mit AWS Organizations

Sie können Security Hub für Konten in Ihrer Organisation integrieren AWS Security Hub und anschließend verwalten. AWS Organizations

Um Security Hub zu integrieren AWS Organizations, erstellen Sie eine Organisation in AWS Organizations. Das Verwaltungskonto der Organizations bestimmt ein Konto als delegierten Security Hub-Administrator für die Organisation. Der delegierte Administrator kann Security Hub dann für andere Konten in der Organisation aktivieren, diese Konten als Security Hub Hub-Mitgliedskonten hinzufügen und zulässige Aktionen für die Mitgliedskonten ausführen. Der delegierte Security Hub-Administrator kann Security Hub für bis zu 10.000 Mitgliedskonten aktivieren und verwalten.

Der Umfang der Konfigurationsmöglichkeiten des delegierten Administrators hängt davon ab, ob Sie die zentrale Konfiguration verwenden. Wenn die zentrale Konfiguration aktiviert ist, müssen Sie Security Hub nicht in jedem Mitgliedskonto separat konfigurieren und AWS-Region. Der delegierte Administrator kann spezifische Security Hub Hub-Einstellungen in bestimmten Mitgliedskonten und Organisationseinheiten (OUs) regionsübergreifend durchsetzen.

Das delegierte Security Hub-Administratorkonto kann die folgenden Aktionen für Mitgliedskonten ausführen:

- Wenn Sie die zentrale Konfiguration verwenden, konfigurieren Sie Security Hub zentral für Mitgliedskonten und Organisationseinheiten, indem Sie Security Hub Hub-Konfigurationsrichtlinien erstellen. Konfigurationsrichtlinien können verwendet werden, um Security Hub zu aktivieren und zu deaktivieren, Standards zu aktivieren und zu deaktivieren und Kontrollen zu aktivieren und zu deaktivieren.
- Behandeln Sie neue Konten automatisch als Security Hub Hub-Mitgliedskonten, wenn sie der Organisation beitreten. Wenn Sie die zentrale Konfiguration verwenden, umfasst eine Konfigurationsrichtlinie, die einer Organisationseinheit zugeordnet ist, bestehende und neue Konten, die Teil der Organisationseinheit sind.
- Behandeln Sie bestehende Unternehmenskonten als Security Hub Hub-Mitgliedskonten. Dies geschieht automatisch, wenn Sie die zentrale Konfiguration verwenden.
- Trennen Sie die Zuordnung von Mitgliedskonten, die zur Organisation gehören. Wenn Sie die zentrale Konfiguration verwenden, können Sie die Zuordnung eines Mitgliedskontos erst aufheben, nachdem Sie es als selbstverwaltet gekennzeichnet haben. Alternativ können Sie

eine Konfigurationsrichtlinie, die Security Hub deaktiviert, bestimmten zentral verwalteten Mitgliedskonten zuordnen.

Eine vollständige Liste der Aktionen, die der delegierte Administrator an Mitgliedskonten durchführen kann, finden Sie unter. Zulässige Aktionen für Konten

In den Themen in diesem Abschnitt wird erklärt, wie Security Hub in Konten in einer Organisation integriert AWS Organizations und verwaltet wird. Wo relevant, werden in jedem Abschnitt die Verwaltungsvorteile und Unterschiede für Benutzer der zentralen Konfiguration aufgeführt.

Themen

Integrieren von Security Hub mit AWS Organizations

Um AWS Security Hub und zu integrieren AWS Organizations, erstellen Sie eine Organisation in Organizations und verwenden das Organisationsverwaltungskonto, um ein delegiertes Security Hub-Administratorkonto zu benennen. Der delegierte Administrator kann dann Security Hub für Mitgliedskonten aktivieren, Daten in Mitgliedskonten anzeigen und andere zulässige Aktionen für Mitgliedskonten ausführen.

Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte Administrator auch Security Hub-Konfigurationsrichtlinien erstellen, die angeben, wie der Security Hub-Service, die Standards und Kontrollen in Organisationskonten konfiguriert werden sollen.

Erstellen einer Organisation

Eine Organisation ist eine Entität, die Sie erstellen, um Ihre zu konsolidieren, AWS-Konten sodass Sie sie als eine einzige Einheit verwalten können.

Sie können eine Organisation erstellen, indem Sie entweder die AWS Organizations Konsole oder einen Befehl aus der AWS CLI oder eine der SDK-APIs verwenden. Detaillierte Anweisungen finden Sie unter Erstellen einer Organisation im AWS Organizations -Benutzerhandbuch.

Sie können verwenden AWS Organizations , um alle Konten in Ihrer Organisation zentral anzuzeigen und zu verwalten. Eine Organisation besteht aus einem Verwaltungskonto und gegebenenfalls Mitgliedskonten. Sie können die Konten in einer hierarchischen, Baumstruktur mit einem Stamm an der Spitze und Organisationseinheiten (OUs) unter dem Stamm anordnen. Jedes Konto kann sich direkt unter dem Stamm befinden oder in einer der OUs in der Hierarchie platziert werden. Eine Organisationseinheit ist ein Container für bestimmte Konten. Sie können beispielsweise eine Finanzorganisationseinheit erstellen, die alle Konten im Zusammenhang mit Finanzoperationen umfasst.

Empfehlungen zur Auswahl des delegierten Security Hub-Administrators

Wenn Sie über ein Administratorkonto aus dem manuellen Einladungsprozess verfügen und zur Kontoverwaltung mit übergehen AWS Organizations, empfiehlt Security Hub, dieses Konto als delegierten Security Hub-Administrator zu bestimmen.

Sie sollten das Organisationsverwaltungskonto nicht als delegierten Security Hub-Administrator festlegen. Dies liegt daran, dass sich Benutzer, die Zugriff auf das Organisationsverwaltungskonto haben, um die Abrechnung zu verwalten, wahrscheinlich von Benutzern unterscheiden, die Zugriff auf Security Hub für das Sicherheitsmanagement benötigen.

Wir empfehlen, denselben delegierten Administrator für alle Regionen zu verwenden. Wenn Sie sich für die zentrale Konfiguration entscheiden, bestimmt Security Hub automatisch denselben delegierten Administrator in Ihrer Heimatregion und allen verknüpften Regionen.

Überprüfen der Berechtigungen zum Konfigurieren des delegierten Security Hub-Administrators

Um ein delegiertes Security Hub-Administratorkonto zu benennen und zu entfernen, muss das Organisationsverwaltungskonto über Berechtigungen für die `DisableOrganizationAdminAccount` Aktionen `EnableOrganizationAdminAccount` und in Security Hub verfügen. Das Verwaltungskonto von Organizations muss auch über Administratorberechtigungen für Organizations verfügen.

Um alle erforderlichen Berechtigungen zu erteilen, fügen Sie dem IAM-Prinzipal für das Verwaltungskonto der Organisation die folgenden verwalteten Security Hub-Richtlinien an:

- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess

Benennen des delegierten Security Hub-Administrators

Um das delegierte Security Hub-Administratorkonto zu bestimmen, können Sie die Security Hub-Konsole, die Security Hub-API oder verwenden AWS CLI. Security Hub legt den delegierten Administrator AWS-Region nur im aktuellen fest, und Sie müssen die Aktion in anderen Regionen wiederholen. Wenn Sie die zentrale Konfiguration verwenden, legt Security Hub automatisch denselben delegierten Administrator in der Heimatregion und den verknüpften Regionen fest.

Das Verwaltungskonto der Organisation muss Security Hub nicht aktivieren, um das delegierte Security-Hub-Administratorkonto zu bestimmen.

Wir empfehlen, dass das Verwaltungskonto der Organisation nicht das delegierte Security Hub-Administratorkonto ist. Wenn Sie jedoch das Organisationsverwaltungskonto als delegierten Security Hub-Administrator auswählen, muss für das Verwaltungskonto Security Hub aktiviert sein. Wenn für das Verwaltungskonto Security Hub nicht aktiviert ist, müssen Sie Security Hub dafür manuell aktivieren. Security Hub kann nicht automatisch für das Verwaltungskonto der Organisation aktiviert werden.

> **Note**
>
> Sie müssen den delegierten Security Hub-Administrator mit einer der folgenden Methoden benennen. Die Benennung des delegierten Security Hub-Administrators mit Organizations-APIs spiegelt sich nicht in Security Hub wider.
> Wählen Sie Ihre bevorzugte Methode aus und folgen Sie den Schritten, um das delegierte Security Hub-Administratorkonto festzulegen.

Security Hub console

So weisen Sie den delegierten Security Hub-Administrator beim Onboarding an

1. Öffnen Sie die - AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie Zu Security Hub gehen aus. Sie werden aufgefordert, sich beim Verwaltungskonto der Organisation anzumelden.
3. Geben Sie auf der Seite Delegierten Administrator festlegen im Abschnitt Delegiertes Administratorkonto das delegierte Administratorkonto an. Wir empfehlen, denselben delegierten Administrator auszuwählen, den Sie für andere AWS Sicherheits- und Compliance-Services festgelegt haben.

4. Wählen Sie Delegierten Administrator festlegen aus. Sie werden aufgefordert, sich beim delegierten Administratorkonto anzumelden (falls noch nicht geschehen), um das Onboarding mit der zentralen Konfiguration fortzusetzen. Wenn Sie die zentrale Konfiguration nicht starten möchten, wählen Sie Abbrechen aus. Ihr delegierter Administrator ist festgelegt, aber Sie verwenden noch keine zentrale Konfiguration.

So weisen Sie den delegierten Security Hub-Administrator auf der Seite Einstellungen an

1. Öffnen Sie die - AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich von Security Hub Einstellungen aus. Wählen Sie dann Allgemein aus.
3. Wenn derzeit ein Security Hub-Administratorkonto zugewiesen ist, müssen Sie das aktuelle Konto entfernen, bevor Sie ein neues Konto festlegen können.

   Wählen Sie unter Delegierter Administrator die Option Entfernen aus, um das aktuelle Konto zu entfernen.
4. Geben Sie die Konto-ID des Kontos ein, das Sie als Security Hub-Administratorkonto festlegen möchten.

   Sie müssen dasselbe Security Hub-Administratorkonto in allen Regionen festlegen. Wenn Sie ein Konto festlegen, das sich von dem in anderen Regionen angegebenen Konto unterscheidet, gibt die Konsole einen Fehler zurück.
5. Wählen Sie Delegate (Delegieren).

Security Hub API

Rufen Sie die EnableOrganizationAdminAccount API über das Verwaltungskonto der Organisation auf. Geben Sie die AWS-Konto ID des delegierten Security Hub-Administratorkontos an.

AWS CLI

Führen Sie den enable-organization-admin-account Befehl über das Verwaltungskonto der Organisation aus. Geben Sie die AWS-Konto ID des delegierten Security Hub-Administratorkontos an.

Beispielbefehl:

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

Entfernen des delegierten Security Hub-Administrators

> **Warning**
>
> Wenn Sie die zentrale Konfiguration verwenden, können Sie die Security Hub-Konsole oder Security Hub-APIs nicht verwenden, um das delegierte Administratorkonto zu ändern oder zu entfernen. Wenn das Verwaltungskonto der Organisation die AWS Organizations Konsole oder AWS Organizations APIs verwendet, um den delegierten Security Hub-Administrator zu ändern oder zu entfernen, stoppt Security Hub automatisch die zentrale Konfiguration und löscht Ihre Konfigurationsrichtlinien und Richtlinienzuordnungen. Mitgliedskonten behalten die Konfigurationen bei, die sie hatten, bevor der delegierte Administrator geändert oder entfernt wurde.

Nur das Verwaltungskonto der Organisation kann das delegierte Security Hub-Administratorkonto entfernen.

Um den delegierten Security Hub-Administrator zu ändern, müssen Sie zuerst das aktuelle delegierte Administratorkonto entfernen und dann ein neues Konto festlegen.

Wenn Sie die Security Hub-Konsole verwenden, um den delegierten Administrator in einer Region zu entfernen, wird er automatisch in allen Regionen entfernt.

Die Security Hub-API entfernt nur das delegierte Security Hub-Administratorkonto aus der Region, in der der API-Aufruf oder -Befehl ausgegeben wird. Sie müssen die Aktion in anderen Regionen wiederholen.

Wenn Sie die Organizations-API verwenden, um das delegierte Security Hub-Administratorkonto zu entfernen, wird es automatisch in allen Regionen entfernt.

Entfernen des delegierten Security Hub-Administrators (Organizations API, AWS CLI)

Sie können Organizations verwenden, um den delegierten Security Hub-Administrator in allen Regionen zu entfernen.

Wenn Sie die zentrale Konfiguration zum Verwalten von Konten verwenden, führt das Entfernen des delegierten Administratorkontos zum Löschen Ihrer Konfigurationsrichtlinien und

Richtlinienzuordnungen. Mitgliedskonten behalten die Konfigurationen bei, die sie hatten, bevor der delegierte Administrator geändert oder entfernt wurde. Diese Konten können jedoch nicht mehr vom entfernten delegierten Administratorkonto verwaltet werden. Sie werden zu selbstverwalteten Konten, die in jeder Region separat konfiguriert werden müssen.

Wählen Sie Ihre bevorzugte Methode aus und folgen Sie den Anweisungen, um das delegierte Security Hub-Administratorkonto mit zu entfernen AWS Organizations.

AWS Organizations API

So entfernen Sie den delegierten Security Hub-Administrator

Rufen Sie die DeregisterDelegatedAdministrator -API auf. Geben Sie die Konto-ID des delegierten Administratorkontos und den Service-Prinzipal für Security Hub an, `securityhub.amazonaws.com`.

AWS CLI

So entfernen Sie den delegierten Security Hub-Administrator

Führen Sie den Befehl deregister-delegated-administrator aus. Geben Sie die Konto-ID des delegierten Administratorkontos und den Service-Prinzipal für Security Hub an, `securityhub.amazonaws.com`.

```
aws organizations deregister-delegated-administrator --account-id <admin account ID>
 --service-principal <Security Hub service principal>
```

Beispiel

```
aws organizations deregister-delegated-administrator --account-id 123456789012 --
service-principal securityhub.amazonaws.com
```

Entfernen des delegierten Security Hub-Administrators (Security Hub-Konsole)

Sie können die Security Hub-Konsole verwenden, um den delegierten Security Hub-Administrator in allen Regionen zu entfernen.

Wenn das delegierte Security Hub-Administratorkonto entfernt wird, werden die Mitgliedskonten vom entfernten delegierten Security Hub-Administratorkonto getrennt.

Security Hub ist weiterhin in den Mitgliedskonten aktiviert. Sie werden zu eigenständigen Konten, bis ein neuer Security Hub-Administrator sie als Mitgliedskonten aktiviert.

Wenn das Verwaltungskonto der Organisation kein aktiviertes Konto in Security Hub ist, verwenden Sie die Option auf der Seite Willkommen beim Security Hub.

So entfernen Sie das delegierte Security Hub-Administratorkonto von der Seite Willkommen beim Security Hub

1. Öffnen Sie die - AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie Zu Security Hub gehen aus.
3. Wählen Sie unter Delegierter Administrator die Option Entfernen aus.

Wenn das Verwaltungskonto der Organisation ein aktiviertes Konto in Security Hub ist, verwenden Sie die Option auf der Registerkarte Allgemein der Seite Einstellungen.

So entfernen Sie das delegierte Security Hub-Administratorkonto von der Seite Einstellungen

1. Öffnen Sie die - AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich des Security Hub die Option Einstellungen aus. Wählen Sie dann Allgemein aus.
3. Wählen Sie unter Delegierter Administrator die Option Entfernen aus.

Entfernen des delegierten Security Hub-Administrators (Security Hub API, AWS CLI)

Sie können die Security Hub-API oder Security Hub-Operationen für verwenden AWS CLI , um den delegierten Security Hub-Administrator zu entfernen. Wenn Sie den delegierten Administrator mit einer dieser Methoden entfernen, wird er nur in der Region entfernt, in der der API-Aufruf oder -Befehl ausgegeben wurde. Security Hub aktualisiert keine anderen Regionen und entfernt nicht das delegierte Administratorkonto in AWS Organizations.

Wählen Sie Ihre bevorzugte Methode aus und gehen Sie wie folgt vor, um das delegierte Security Hub-Administratorkonto bei Security Hub zu entfernen.

Security Hub API

So entfernen Sie den delegierten Security Hub-Administrator

Rufen Sie die DisableOrganizationAdminAccount API mit den Anmeldeinformationen des Organisationsverwaltungskontos auf. Geben Sie die Konto-ID des delegierten Security Hub-Administratorkontos an.

AWS CLI

So entfernen Sie den delegierten Security Hub-Administrator

Führen Sie mit den Anmeldeinformationen des Organisationsverwaltungskontos den disable-organization-admin-account Befehl aus. Geben Sie die Konto-ID des delegierten Security Hub-Administratorkontos an.

```
aws securityhub disable-organization-admin-account --admin-account-id <admin account
 ID>
```

Beispiel

```
aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

Automatisches Aktivieren von Security Hub in neuen Unternehmenskonten

Wenn neue Konten Ihrer Organisation beitreten, werden sie der Liste auf der Kontoseite der AWS Security Hub Konsole hinzugefügt. Für Organisationskonten lautet Typ auf Nach Organisation. Standardmäßig werden neue Konten nicht zu Security Hub Hub-Mitgliedern, wenn sie der Organisation beitreten. Ihr Status ist Kein Mitglied. Das delegierte Administratorkonto kann automatisch neue Konten als Mitglieder hinzufügen und Security Hub in diesen Konten aktivieren, wenn sie der Organisation beitreten.

> **Note**
>
> Obwohl viele Regionen standardmäßig für Sie aktiv AWS-Regionen sind AWS-Konto, müssen Sie bestimmte Regionen manuell aktivieren. Diese Regionen werden in diesem Dokument als Opt-in-Regionen bezeichnet. Um Security Hub automatisch in einem neuen Konto in einer Opt-in-Region zu aktivieren, muss diese Region zuerst für das Konto aktiviert sein. Nur der Kontoinhaber kann die Opt-in-Region aktivieren. Weitere Informationen zu Opt-in-Regionen finden Sie unter Geben Sie an, welche Regionen AWS-Regionen Ihr Konto verwenden kann.

Dieser Vorgang unterscheidet sich je nachdem, ob Sie die zentrale Konfiguration (empfohlen) oder die lokale Konfiguration verwenden.

Automatische Aktivierung neuer Organisationskonten (zentrale Konfiguration)

Wenn Sie die zentrale Konfiguration verwenden, können Sie Security Hub automatisch in neuen und bestehenden Unternehmenskonten aktivieren, indem Sie eine Konfigurationsrichtlinie erstellen, in der Security Hub aktiviert ist. Anschließend können Sie die Richtlinie dem Organisationsstamm oder bestimmten Organisationseinheiten (OUs) zuordnen.

Wenn Sie eine Konfigurationsrichtlinie, in der Security Hub aktiviert ist, einer bestimmten OU zuordnen, wird Security Hub automatisch in allen Konten (vorhandenen und neuen) aktiviert, die zu dieser OU gehören. Neue Konten, die nicht zur Organisationseinheit gehören, werden selbst verwaltet und Security Hub ist nicht automatisch aktiviert. Wenn Sie dem Root eine Konfigurationsrichtlinie zuordnen, in der Security Hub aktiviert ist, wird Security Hub automatisch in allen Konten (bestehenden und neuen) aktiviert, die der Organisation beitreten. Ausnahmen sind, wenn ein Konto aufgrund von Anwendung oder Vererbung eine andere Richtlinie verwendet oder wenn es sich um ein selbstverwaltetes Konto handelt.

In Ihrer Konfigurationsrichtlinie können Sie auch definieren, welche Sicherheitsstandards und Kontrollen in der Organisationseinheit aktiviert werden sollen. Um Kontrollergebnisse für aktivierte Standards zu generieren, müssen die Konten in der Organisationseinheit AWS Config aktiviert und konfiguriert sein, um die erforderlichen Ressourcen aufzuzeichnen. Weitere Informationen zur AWS Config Aufzeichnung finden Sie unter Aktivieren und Konfigurieren AWS Config.

Anweisungen zum Erstellen einer Konfigurationsrichtlinie finden Sie unterSecurity Hub Hub-Konfigurationsrichtlinien erstellen und zuordnen.

Automatisches Aktivieren neuer Organisationskonten (lokale Konfiguration)

Wenn Sie die lokale Konfiguration verwenden und die automatische Aktivierung aktivieren, fügt Security Hub neue Organisationskonten als Mitglieder hinzu und aktiviert Security Hub in diesen Konten in der aktuellen Region. Andere Regionen sind nicht betroffen. Darüber hinaus aktiviert die Aktivierung der automatischen Aktivierung Security Hub nicht für bestehende Unternehmenskonten, es sei denn, sie wurden bereits als Mitgliedskonten hinzugefügt.

Nach der Aktivierung der automatischen Aktivierung werden die Standardsicherheitsstandards auch automatisch für neue Konten in der aktuellen Region aktiviert, wenn sie der Organisation beitreten. Die Standardstandards sind AWS Foundational Security Best Practices (FSBP) und Center for

Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Sie können die Standardstandards nicht ändern. Wenn Sie andere Standards in Ihrer Organisation aktivieren oder Standards für ausgewählte Konten und Organisationseinheiten aktivieren möchten, empfehlen wir die zentrale Konfiguration.

Um Kontrollergebnisse für die Standardstandards (und andere aktivierte Standards) zu generieren, müssen die Konten in Ihrer Organisation AWS Config aktiviert und konfiguriert sein, um die erforderlichen Ressourcen aufzuzeichnen. Weitere Informationen zur AWS Config Aufzeichnung finden Sie unter Aktivieren und Konfigurieren AWS Config.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um Security Hub automatisch in neuen Unternehmenskonten zu aktivieren. Diese Anweisungen gelten nur, wenn Sie die lokale Konfiguration verwenden.

Security Hub console

So aktivieren Sie automatisch neue Organisationskonten als Security Hub Hub-Mitglieder

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

   Sign verwendet die Anmeldeinformationen des delegierten Administratorkontos.
2. Wählen Sie im Security Hub-Navigationsbereich unter Einstellungen die Option Konfiguration aus.
3. Aktivieren Sie im Bereich Konten die Option Konten automatisch aktivieren.

Security Hub API

So aktivieren Sie automatisch neue Organisationskonten als Security Hub Hub-Mitglieder

Rufen Sie die `UpdateOrganizationConfiguration`API vom delegierten Administratorkonto aus auf. Setzen Sie das `AutoEnable` Feld auf, `true` um Security Hub automatisch in neuen Organisationskonten zu aktivieren.

AWS CLI

So aktivieren Sie automatisch neue Organisationskonten als Security Hub Hub-Mitglieder

Führen Sie den `update-organization-configuration`Befehl über das delegierte Administratorkonto aus. Fügen Sie den `auto-enable` Parameter hinzu, um Security Hub automatisch in neuen Organisationskonten zu aktivieren.

```
aws securityhub update-organization-configuration --auto-enable
```

Manuelles Aktivieren von Security Hub in neuen Unternehmenskonten

Wenn Sie Security Hub nicht automatisch in neuen Organisationskonten aktivieren, wenn sie der Organisation beitreten, können Sie diese Konten als Mitglieder hinzufügen und Security Hub in ihnen manuell aktivieren, nachdem sie der Organisation beigetreten sind. Sie müssen Security Hub auch manuell aktivieren AWS-Konten , wenn Sie zuvor die Verbindung zu einer Organisation getrennt haben.

> **Note**
>
> Dieser Abschnitt gilt nicht für Sie, wenn Sie die zentrale Konfiguration verwenden. Wenn Sie die zentrale Konfiguration verwenden, können Sie Konfigurationsrichtlinien erstellen, die Security Hub in bestimmten Mitgliedskonten und Organisationseinheiten (OUs) aktivieren. Sie können auch spezifische Standards und Kontrollen für diese Konten und Organisationseinheiten aktivieren.

Sie können Security Hub nicht in einem Konto aktivieren, wenn es sich bereits um ein Mitgliedskonto in einer anderen Organisation handelt.

Sie können Security Hub auch nicht in einem Konto aktivieren, das derzeit gesperrt ist. Wenn Sie versuchen, den Dienst in einem gesperrten Konto zu aktivieren, ändert sich der Kontostatus in Konto gesperrt.

- Wenn Security Hub für das Konto nicht aktiviert ist, ist Security Hub in diesem Konto aktiviert. Der Standard AWS Foundational Security Best Practices (FSBP) und der CIS AWS Foundations Benchmark v1.2.0 sind ebenfalls im Konto aktiviert, sofern Sie die Standardsicherheitsstandards nicht deaktivieren.

  Eine Ausnahme bildet das Verwaltungskonto für Organizations. Security Hub kann nicht automatisch im Verwaltungskonto der Organizations aktiviert werden. Sie müssen Security Hub manuell im Verwaltungskonto der Organizations aktivieren, bevor Sie es als Mitgliedskonto hinzufügen können.
- Wenn Security Hub für das Konto bereits aktiviert ist, nimmt Security Hub keine weiteren Änderungen am Konto vor. Es aktiviert nur die Mitgliedschaft.

Damit Security Hub Kontrollergebnisse generieren kann, müssen Mitgliedskonten AWS Config aktiviert und konfiguriert sein, um die erforderlichen Ressourcen aufzuzeichnen. Weitere Informationen zur Konfiguration von SSH finden Sie unter Aktivieren und Konfigurieren von AWS Config.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um ein Organisationskonto als Security Hub-Mitgliedskonto zu aktivieren.

Security Hub console

Um Unternehmenskonten manuell als Security Hub Hub-Mitglieder zu aktivieren

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit den Anmeldeinformationen des delegierten Administratorkontos an.
2. Wählen Sie im Security Hub-Navigationsbereich unter Einstellungen die Option Konfiguration aus.
3. Wählen Sie in der Kontenliste jedes Unternehmenskonto aus, das Sie aktivieren möchten.
4. Wählen Sie Aktionen und dann Mitglied hinzufügen aus.

Security Hub API

Um Unternehmenskonten manuell als Security Hub Hub-Mitglieder zu aktivieren

Rufen Sie die `CreateMembers`API vom delegierten Administratorkonto aus auf. Geben Sie für jedes zu aktivierende Konto die Konto-ID an.

Im Gegensatz zum manuellen Einladungsprozess müssen `CreateMembers` Sie bei der Aktivierung eines Unternehmenskontos keine Einladung versenden.

AWS CLI

Um Unternehmenskonten manuell als Security Hub Hub-Mitglieder zu aktivieren

Führen Sie den `create-members`Befehl über das delegierte Administratorkonto aus. Geben Sie für jedes zu aktivierende Konto die Konto-ID an.

Im Gegensatz zum manuellen Einladungsprozess `create-members` müssen Sie bei der Aktivierung eines Unternehmenskontos keine Einladung versenden.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

Beispiel

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

Aufheben der Zuordnung von Mitgliedskonten zu Ihrer Organisation

Wenn Sie keine Ergebnisse von einem AWS Security Hub Mitgliedskonto mehr empfangen und einsehen möchten, können Sie die Verknüpfung des Mitgliedskontos mit Ihrer Organisation trennen.

> **Note**
>
> Wenn Sie die zentrale Konfiguration verwenden, funktioniert die Trennung anders. Sie können eine Konfigurationsrichtlinie erstellen, die Security Hub in einem oder mehreren zentral verwalteten Mitgliedskonten deaktiviert. Danach sind diese Konten immer noch Teil der Organisation, generieren aber keine Security Hub Hub-Ergebnisse. Wenn Sie die zentrale Konfiguration verwenden, aber auch über manuell eingeladene Mitgliedskonten verfügen, können Sie die Zuordnung zu einem oder mehreren manuell eingeladenen Konten aufheben.

Mitgliedskonten, die über verwaltet werden, AWS Organizations können ihre Konten nicht vom Administratorkonto trennen. Nur das Administratorkonto kann die Zuordnung eines Mitgliedskontos aufheben.

Durch das Aufheben der Zuordnung zu einem Mitgliedskonto wird das Konto nicht geschlossen. Stattdessen wird das Mitgliedskonto aus der Organisation entfernt. Das getrennte Mitgliedskonto wird zu einem eigenständigen Konto AWS-Konto , das nicht mehr über die Security Hub Hub-Integration mit AWS Organizations verwaltet wird.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um ein Mitgliedskonto von der Organisation zu trennen.

Security Hub console

Um ein Mitgliedskonto von der Organisation zu trennen

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit den Anmeldeinformationen des delegierten Administratorkontos an.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Konfiguration aus.
3. Wählen Sie im Abschnitt Konten die Konten aus, deren Verknüpfung Sie aufheben möchten. Wenn Sie die zentrale Konfiguration verwenden, können Sie auf der Registerkarte ein manuell eingerichtetes Konto auswählen, dessen Verknüpfung aufgehoben werden soll. `Invitation accounts` Diese Registerkarte ist nur sichtbar, wenn Sie die zentrale Konfiguration verwenden.
4. Wählen Sie Aktionen und anschließend Konto trennen aus.

Security Hub API

Um ein Mitgliedskonto von der Organisation zu trennen

Rufen Sie die `DisassociateMembers`API vom delegierten Administratorkonto aus auf. Sie müssen die AWS-Konto IDs für die Mitgliedskonten angeben, um die Zuordnung aufzuheben. Rufen Sie die API auf, um eine Liste der Mitgliedskonten anzuzeigen. `ListMembers`

AWS CLI

Um ein Mitgliedskonto von der Organisation zu trennen

Führen Sie den `disassociate-members` Befehl > vom delegierten Administratorkonto aus. Sie müssen die AWS-Konto IDs für die Mitgliedskonten angeben, um die Zuordnung aufzuheben. Um eine Liste der Mitgliedskonten anzuzeigen, führen Sie den `list-members` Befehl > aus.

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

Beispiel

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Sie können auch die AWS Organizations Konsole oder AWS SDKs verwenden AWS CLI, um die Zuordnung eines Mitgliedskontos zu Ihrer Organisation aufzuheben. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Entfernen eines Mitgliedskontos aus Ihrer Organisation.

Deaktivieren der Security Hub Hub-Integration mit AWS Organizations

Nachdem eine AWS Organizations Organisation integriert wurde AWS Security Hub, kann das Verwaltungskonto der Organizations die Integration anschließend deaktivieren. Als Benutzer des Organisationsverwaltungskontos können Sie dies tun, indem Sie den vertrauenswürdigen Zugriff für Security Hub in AWS Organizations deaktivieren.

Wenn Sie den vertrauenswürdigen Zugriff für Security Hub deaktivieren, passiert Folgendes:

- Security Hub verliert seinen Status als vertrauenswürdiger Dienst in AWS Organizations.
- Das delegierte Security Hub-Administratorkonto verliert den Zugriff auf Security Hub Hub-Einstellungen, Daten und Ressourcen für alle Security Hub Hub-Mitgliedskonten insgesamt. AWS-Regionen
- Wenn Sie die zentrale Konfiguration verwendet haben, verwendet Security Hub sie automatisch nicht mehr für Ihr Unternehmen. Ihre Konfigurationsrichtlinien und Richtlinienverknüpfungen werden gelöscht. Konten behalten die Konfigurationen bei, die sie hatten, bevor Sie den vertrauenswürdigen Zugriff deaktiviert haben.
- Alle Security Hub Hub-Mitgliedskonten werden zu eigenständigen Konten und behalten ihre aktuellen Einstellungen bei. Wenn Security Hub für ein Mitgliedskonto in einer oder mehreren Regionen aktiviert wurde, ist Security Hub weiterhin für das Konto in diesen Regionen aktiviert. Die aktivierten Standards und Kontrollen bleiben ebenfalls unverändert. Sie können diese Einstellungen für jedes Konto und jede Region separat ändern. Das Konto ist jedoch in keiner Region mehr einem delegierten Administrator zugeordnet.

Weitere Informationen zu den Ergebnissen der Deaktivierung des Zugriffs auf vertrauenswürdige Dienste finden Sie AWS-Services im AWS Organizations Benutzerhandbuch unter AWS Organizations Zusammen mit anderen Benutzern verwenden.

Um den vertrauenswürdigen Zugriff zu deaktivieren, können Sie die AWS Organizations Konsole, die Organisations-API oder die verwenden AWS CLI. Nur ein Benutzer des Organisationsverwaltungskontos kann den vertrauenswürdigen Dienstzugriff für Security Hub deaktivieren. Einzelheiten zu den Berechtigungen, die Sie benötigen, finden Sie im AWS

Organizations Benutzerhandbuch unter Erforderliche Berechtigungen zur Deaktivierung des vertrauenswürdigen Zugriffs.

Bevor Sie den vertrauenswürdigen Zugriff deaktivieren, empfehlen wir, mit dem delegierten Administrator Ihrer Organisation zusammenzuarbeiten, um Security Hub in Mitgliedskonten zu deaktivieren und die Security Hub Hub-Ressourcen in diesen Konten zu bereinigen.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um den vertrauenswürdigen Zugriff für Security Hub zu deaktivieren.

Organizations console

So deaktivieren Sie den vertrauenswürdigen Zugriff für Security Hub

1. Melden Sie sich AWS Management Console mit den Anmeldeinformationen des AWS Organizations Verwaltungskontos an.
2. Öffnen Sie die Organisationskonsole unter https://console.aws.amazon.com/organizations/.
3. Wählen Sie im Navigationsbereich Services.
4. Wählen Sie unter Integrierte Dienste die Option AWS Security Hub.
5. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
6. Bestätigen Sie, dass Sie den vertrauenswürdigen Zugriff deaktivieren möchten.

Organizations API

So deaktivieren Sie den vertrauenswürdigen Zugriff für Security Hub

Rufen Sie den AWSServiceAccess Deaktivierungsvorgang der AWS Organizations API auf. Geben Sie für den `ServicePrincipal` Parameter den Security Hub Hub-Dienstprinzipal (`securityhub.amazonaws.com`) an.

AWS CLI

So deaktivieren Sie den vertrauenswürdigen Zugriff für Security Hub

Führen Sie den disable-aws-service-accessBefehl der AWS Organizations API aus. Geben Sie für den `service-principal` Parameter den Security Hub Hub-Dienstprinzipal (`securityhub.amazonaws.com`) an.

Beispiel:

```
aws organizations disable-aws-service-access --service-principal
 securityhub.amazonaws.com
```

Verwalten von Konten auf Einladung

Sie können mehrere AWS Security Hub Konten auf zwei Arten zentral verwalten, indem Sie Security Hub in Security Hub integrieren AWS Organizations oder indem Sie Mitgliedschaftseinladungen manuell senden und annehmen. Sie müssen den manuellen Prozess verwenden, wenn Sie ein eigenständiges Konto haben oder wenn Sie keine Integration mit Organizations durchführen. Bei der manuellen Kontoverwaltung lädt der Security Hub-Administrator Konten ein, Mitglieder zu werden. Die Beziehung zwischen Administrator und Mitglied wird hergestellt, wenn ein potenzielles Mitglied die Einladung annimmt. Ein Security Hub-Administratorkonto kann Security Hub für bis zu 1.000 Mitgliedskonten verwalten, die auf Einladung basieren.

> **Tip**
>
> Wenn Sie in Security Hub eine Organisation erstellen, die auf Einladung basiert, können Sie anschließend auf die Verwendung AWS Organizations umsteigen. Wenn Sie mehr als ein Mitgliedskonto haben, empfehlen wir, Konten über zu verwalten. AWS Organizations

Für Konten, die Sie über den manuellen Einladungsprozess einladen, ist eine regionsübergreifende Aggregation von Ergebnissen und anderen Daten verfügbar. Der Administrator muss jedoch das Mitgliedskonto aus der Aggregationsregion und allen verknüpften Regionen einladen, damit die regionsübergreifende Aggregation funktioniert. Darüber hinaus muss Security Hub für das Mitgliedskonto in der Aggregationsregion und allen verknüpften Regionen aktiviert sein, damit der Administrator die Ergebnisse des Mitgliedskontos einsehen kann.

Konfigurationsrichtlinien werden für manuell eingeladene Mitgliedskonten nicht unterstützt. Stattdessen müssen Sie die Security Hub Hub-Einstellungen in jedem Mitgliedskonto und AWS-Region bei Verwendung des manuellen Einladungsprozesses separat konfigurieren.

Sie müssen den manuellen Einladungsprozess auch für Konten verwenden, die nicht zu Ihrer Organisation gehören. Beispielsweise könnten Sie in Ihrer Organisation kein Testkonto einrichten. Oder vielleicht möchten Sie Konten mehrerer Organisationen unter einem einzigen Security Hub-Administratorkonto konsolidieren. Das Security Hub-Administratorkonto muss Einladungen an Konten senden, die anderen Organisationen gehören.

Auf der Konfigurationsseite der Security Hub Hub-Konsole werden Konten, die auf Einladung hinzugefügt wurden, auf der Registerkarte Einladungskonten aufgeführt. Wenn Sie Konten außerhalb Ihrer Organisation verwendenSo funktioniert die zentrale Konfiguration, aber auch Konten einladen, können Sie sich auf dieser Registerkarte die Ergebnisse von Konten ansehen, die auf Einladungen basieren. Der Security Hub-Administrator kann jedoch mithilfe von Konfigurationsrichtlinien keine Konten, die auf Einladungen basieren, regionsübergreifend konfigurieren.

In den Themen in diesem Abschnitt wird erklärt, wie Mitgliedskonten mithilfe von Einladungen verwaltet werden.

Themen

Mitgliedskonten hinzufügen und einladen

Ihr Konto wird zum AWS Security Hub Administrator für Konten, die Ihre Einladung annehmen.

Wenn Sie eine Einladung von einem anderen Konto annehmen, wird Ihr Konto zu einem Mitgliedskonto und dieses Konto wird zu Ihrem Administrator.

Wenn es sich bei Ihrem Konto um ein Administratorkonto handelt, können Sie eine Einladung, ein Mitgliedskonto zu werden, nicht annehmen.

Das Hinzufügen eines Mitgliedskontos besteht aus den folgenden Schritten:

1. Das Administratorkonto fügt das Mitgliedskonto zu seiner Liste der Mitgliedskonten hinzu.
2. Das Administratorkonto sendet eine Einladung an das Mitgliedskonto.
3. Das Mitgliedskonto akzeptiert die Einladung.

Mitgliedskonten hinzufügen

Von der Security Hub Hub-Konsole aus können Sie Konten zu Ihrer Liste der Mitgliedskonten hinzufügen. In der Security Hub Hub-Konsole können Sie Konten einzeln auswählen oder eine `.csv` Datei hochladen, die die Kontoinformationen enthält.

Für jedes Konto müssen Sie die Konto-ID und eine E-Mail-Adresse angeben. Die E-Mail-Adresse sollte die E-Mail-Adresse sein, an die Sie sich bei Sicherheitsproblemen im Konto wenden können. Sie wird nicht zur Verifizierung des Kontos verwendet.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zum Hinzufügen von Mitgliedskonten.

Security Hub console

Um Konten zu deiner Liste von Mitgliedskonten hinzuzufügen

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit den Anmeldeinformationen des Administratorkontos an.
2. Wählen Sie im linken Bereich Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Option Konten und dann Konten hinzufügen aus. Sie können dann entweder einzelne Konten hinzufügen oder eine `.csv` Datei hochladen, die die Liste der Konten enthält.
4. Gehen Sie wie folgt vor, um die Konten auszuwählen:

   - Um die Konten einzeln hinzuzufügen, geben Sie unter Konten eingeben die Konto-ID und die E-Mail-Adresse des hinzuzufügenden Kontos ein, und wählen Sie dann Hinzufügen aus.

     Wiederholen Sie diesen Vorgang für jedes Konto.
   - Um eine Datei mit kommagetrennten Werten (.csv) zum Hinzufügen mehrerer Konten zu verwenden, erstellen Sie zunächst die Datei. Die Datei muss die Konto-ID und die E-Mail-Adresse für jedes hinzuzufügende Konto enthalten.

     In Ihrer `.csv` Liste muss eines pro Zeile erscheinen. Die erste Zeile der `.csv` Datei muss den Header enthalten. In der Kopfzeile befindet sich die erste Spalte **`Account ID`** und die zweite Spalte**`Email`**.

Jede weitere Zeile muss eine gültige Konto-ID und eine gültige E-Mail-Adresse für das Konto enthalten, das Sie hinzufügen möchten.

Hier ist ein Beispiel für eine `.csv` Datei, wenn sie in einem Texteditor angezeigt wird.

```
Account ID,Email
111111111111,user@example.com
```

In einem Tabellenkalkulationsprogramm werden die Felder in separaten Spalten angezeigt. Das zugrunde liegende Format ist immer noch durch Kommas getrennt. Sie müssen die Konto-IDs als Zahlen ohne Dezimalzahlen formatieren. Beispielsweise kann die Konto-ID 444455556666 nicht als 444455556666.0 formatiert werden. Stellen Sie außerdem sicher, dass bei der Zahlenformatierung keine führenden Nullen aus der Konto-ID entfernt werden.

Um die Datei auszuwählen, wählen Sie auf der Konsole die Option Liste hochladen (.csv). Wählen Sie dann „Durchsuchen“.

Nachdem Sie die Datei ausgewählt haben, wählen Sie Konten hinzufügen.

5. Wenn Sie mit dem Hinzufügen von Konten fertig sind, wählen Sie unter Hinzuzufügende Konten die Option Weiter aus.

Security Hub API

Um Konten zu Ihrer Liste von Mitgliedskonten hinzuzufügen

Rufen Sie die `CreateMembers`API vom Administratorkonto aus auf. Für jedes Mitgliedskonto, das hinzugefügt werden soll, müssen Sie die AWS-Konto ID angeben.

AWS CLI

Um Konten zu Ihrer Liste von Mitgliedskonten hinzuzufügen

Führen Sie den `create-members`Befehl vom Administratorkonto aus. Für jedes Mitgliedskonto, das hinzugefügt werden soll, müssen Sie die AWS-Konto ID angeben.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

Beispiel

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

Laden Sie Mitgliedskonten ein

Nachdem Sie die Mitgliedskonten hinzugefügt haben, senden Sie eine Einladung an das Mitgliedskonto. Sie können eine Einladung auch erneut an ein Konto senden, das Sie vom Administrator getrennt haben.

Security Hub console

Um Konten potenzieller Mitglieder einzuladen

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit den Anmeldeinformationen des Administratorkontos an.
2. Wählen Sie im Navigationsbereich Einstellungen und dann Konten aus.
3. Wählen Sie für das einzuladende Konto Invite (Einladen) in der Spalte Status aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Einladen aus.

> **Note**
>
> Um Einladungen an getrennte Konten erneut zu senden, wählen Sie auf der Seite Konten jedes getrennte Konto aus. Wählen Sie unter Aktionen die Option Einladung erneut senden aus.

Security Hub API

Um Konten potenzieller Mitglieder einzuladen

Rufen Sie die `InviteMembers`API vom Administratorkonto aus auf. Für jedes Konto, das eingeladen werden soll, müssen Sie die AWS-Konto ID angeben.

AWS CLI

Um Konten potenzieller Mitglieder einzuladen

Führen Sie den `invite-members`Befehl vom Administratorkonto aus. Für jedes Konto, das eingeladen werden soll, müssen Sie die AWS-Konto ID angeben.

```
aws securityhub invite-members --account-ids <accountIDs>
```

Beispiel

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

Auf eine Einladung zur Registrierung als Mitgliedskonto antworten

Sie können eine Einladung zur Registrierung als Mitgliedskonto annehmen oder ablehnen.

Nachdem Sie eine Einladung angenommen haben, wird Ihr Konto zu einem AWS Security Hub Mitgliedskonto. Das Konto, das die Einladung gesendet hat, wird zu Ihrem Security Hub-Administratorkonto. Der Benutzer des Administratorkontos kann die Ergebnisse für Ihr Mitgliedskonto in Security Hub einsehen.

Wenn Sie die Einladung ablehnen, wird Ihr Konto in der Liste der Mitgliedskonten des Administratorkontos als Abgemeldet markiert.

Sie können nur eine Einladung annehmen, ein Mitgliedskonto zu werden.

Bevor Sie eine Einladung annehmen oder ablehnen können, müssen Sie Security Hub aktivieren.

Denken Sie daran, dass alle Security Hub Hub-Konten AWS Config aktiviert und konfiguriert sein müssen, um alle Ressourcen aufzuzeichnen. Einzelheiten zu den Anforderungen für AWS Config finden Sie unter Aktivierung und Konfiguration AWS Config.

Nehmen Sie eine Einladung an

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um eine Einladung als Mitgliedskonto anzunehmen.

Security Hub console

Um eine Einladung zur Mitgliedschaft anzunehmen

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

2. Wählen Sie im Navigationsbereich Einstellungen und dann Konten aus.
3. Aktivieren Sie im Abschnitt Administratorkonto die Option Annehmen und wählen Sie dann Einladung annehmen aus.

Security Hub API

Um eine Einladung zur Mitgliedschaft anzunehmen

Rufen Sie die `AcceptAdministratorInvitation`API auf. Sie müssen die Einladungs-ID und die AWS-Konto ID des Administratorkontos angeben. Verwenden Sie den `ListInvitations`Vorgang, um Details zur Einladung abzurufen.

AWS CLI

Um eine Einladung zur Mitgliedschaft anzunehmen

Führen Sie den Befehl `accept-administrator-invitation` aus. Sie müssen die Einladungs-ID und die AWS-Konto ID des Administratorkontos angeben. Führen Sie den `list-invitations`Befehl aus, um Details zur Einladung abzurufen.

```
aws securityhub accept-administrator-invitation --administrator-
id <administratorAccountID> --invitation-id <invitationID>
```

Beispiel

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --
invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

> **Note**
>
> Die Security Hub Hub-Konsole wird weiterhin verwendet`AcceptInvitation`. Sie wird irgendwann auf Verwendung umgestellt`AcceptAdministratorInvitation`. Alle IAM-Richtlinien, die speziell den Zugriff auf diese Funktion steuern, müssen weiterhin verwendet `AcceptInvitation` werden. Sie sollten Ihre Richtlinien auch ergänzen`AcceptAdministratorInvitation`, um sicherzustellen, dass nach Beginn der Nutzung `AcceptAdministratorInvitation` der Konsole die richtigen Berechtigungen vorhanden sind.

Eine Einladung ablehnen

Sie können eine Einladung, ein Mitgliedskonto zu werden, ablehnen. Wenn Sie eine Einladung in der Security Hub Hub-Konsole ablehnen, wird Ihr Konto in der Liste der Mitgliedskonten des Administratorkontos als Signiert markiert.

Wenn Sie eine Einladung ablehnen, müssen Sie bei dem Mitgliedskonto angemeldet sein, das die Einladung erhalten hat.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um eine Einladung als Mitgliedskonto abzulehnen.

Security Hub console

Um eine Einladung zur Mitgliedschaft abzulehnen

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Einstellungen und dann Konten aus.
3. Wählen Sie im Abschnitt Administratorkonto die Option Einladung ablehnen aus.

Security Hub API

Um eine Einladung zur Mitgliedschaft abzulehnen

Rufen Sie die `DeclineInvitations`API auf. Sie müssen die AWS-Konto ID des Administratorkontos angeben, das die Einladung ausgestellt hat. Verwenden Sie den `ListInvitations`Vorgang, um Informationen zu Ihren Einladungen anzuzeigen.

AWS CLI

Um eine Einladung zur Mitgliedschaft abzulehnen

Führen Sie den Befehl `decline-invitations` aus. Sie müssen die AWS-Konto ID des Administratorkontos angeben, das die Einladung ausgestellt hat. Führen Sie den `list-invitations`Befehl aus, um Informationen zu Ihren Einladungen anzuzeigen.

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

Beispiel

```
aws securityhub decline-invitations --account-ids "123456789012"
```

Aufheben der Zuordnung von Mitgliedskonten

Ein AWS Security Hub Administratorkonto kann die Zuordnung zu einem Mitgliedskonto aufheben, sodass keine Ergebnisse mehr von diesem Konto empfangen und angezeigt werden. Sie müssen die Zuordnung zu einem Mitgliedskonto aufheben, bevor Sie es löschen können.

Wenn Sie die Zuordnung zu einem Mitgliedskonto aufheben, verbleibt es in Ihrer Liste der Mitgliedskonten mit dem Status Entfernt (Getrennt). Ihr Konto wird aus den Administratorkontoinformationen für das Mitgliedskonto entfernt.

Um weiterhin Ergebnisse für das Konto zu erhalten, können Sie die Einladung erneut versenden. Um das Mitgliedskonto vollständig zu entfernen, können Sie das Mitgliedskonto löschen.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um ein manuell eingeladenes Mitgliedskonto vom Administratorkonto zu trennen.

Security Hub console

So trennen Sie die Zuordnung eines manuell eingeladenen Mitgliedskontos

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit den Anmeldeinformationen des Administratorkontos an.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Konfiguration aus.
3. Wählen Sie im Abschnitt Konten die Konten aus, deren Verknüpfung Sie aufheben möchten.
4. Wählen Sie „Aktionen“ und anschließend „Konto trennen“.

Security Hub API

Um die Verbindung zu einem manuell eingeladenen Mitgliedskonto zu trennen

Rufen Sie die `DisassociateMembers`API vom Administratorkonto aus auf. Sie müssen die AWS-Konto IDs der Mitgliedskonten angeben, deren Zuordnung Sie aufheben möchten. Verwenden Sie den `ListMembers`Vorgang, um eine Liste der Mitgliedskonten anzuzeigen.

AWS CLI

Um die Zuordnung zu einem manuell eingeladenen Mitgliedskonto aufzuheben

Führen Sie den `disassociate-members`Befehl vom Administratorkonto aus. Sie müssen die AWS-Konto IDs der Mitgliedskonten angeben, deren Zuordnung Sie aufheben möchten. Führen Sie den `list-members`Befehl aus, um eine Liste der Mitgliedskonten anzuzeigen.

```
aws securityhub disassociate-members --account-ids <accountIds>
```

Beispiel

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Mitgliedskonten löschen

Als AWS Security Hub Administratorkonto können Sie Mitgliedskonten löschen, die auf Einladung hinzugefügt wurden. Bevor Sie ein aktiviertes Konto löschen können, müssen Sie die Verknüpfung mit dem Konto aufheben.

Wenn Sie ein Mitgliedskonto löschen, wird es vollständig aus der Liste entfernt. Um die Mitgliedschaft des Kontos wiederherzustellen, müssen Sie es hinzufügen und erneut einladen, als ob es sich um ein völlig neues Mitgliedskonto handeln würde.

Sie können keine Konten löschen, die zu einer Organisation gehören und die mithilfe der Integration mit verwaltet werden AWS Organizations.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zum Löschen manuell eingeladener Mitgliedskonten.

Security Hub console

Um ein manuell eingeladenes Mitgliedskonto zu löschen

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit dem Administratorkonto an.
2. Wählen Sie im Navigationsbereich Einstellungen und dann Konfiguration aus.

3. Wählen Sie den Tab Einladungskonten aus. Wählen Sie dann die Konten aus, die Sie löschen möchten.
4. Wählen Sie Aktionen und anschließend Löschen aus. Diese Option ist nur verfügbar, wenn Sie die Kontoverknüpfung aufgehoben haben. Sie müssen die Zuordnung zu einem Mitgliedskonto aufheben, bevor es gelöscht werden kann.

Security Hub API

Um ein manuell eingeladenes Mitgliedskonto zu löschen

Rufen Sie die `DeleteMembers`API vom Administratorkonto aus auf. Sie müssen die AWS-Konto IDs der Mitgliedskonten angeben, die Sie löschen möchten. Rufen Sie die `ListMembers`API auf, um die Liste der Mitgliedskonten abzurufen.

AWS CLI

Um ein manuell eingeladenes Mitgliedskonto zu löschen

Führen Sie den `delete-members`Befehl vom Administratorkonto aus. Sie müssen die AWS-Konto IDs der Mitgliedskonten angeben, die Sie löschen möchten. Führen Sie den `list-members`Befehl aus, um die Liste der Mitgliedskonten abzurufen.

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

Beispiel

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

Trennen der Verbindung zu Ihrem Administratorkonto

Wenn Ihr Konto auf Einladung als AWS Security Hub Mitgliedskonto hinzugefügt wurde, können Sie die Verknüpfung zwischen dem Mitgliedskonto und dem Administratorkonto trennen. Sobald Sie die Zuordnung zu einem Mitgliedskonto aufheben, sendet Security Hub keine Ergebnisse aus dem Konto an das Administratorkonto.

Mitgliedskonten, die mithilfe der Integration mit verwaltet werden, AWS Organizations können ihre Konten nicht vom Administratorkonto trennen. Nur der delegierte Security Hub-Administrator kann die Zuordnung von Mitgliedskonten aufheben, die mit Organizations verwaltet werden.

Wenn Sie die Verbindung zu Ihrem Administratorkonto trennen, verbleibt Ihr Konto in der Mitgliederliste des Administratorkontos mit dem Status Kündigt. Das Administratorkonto erhält jedoch keine Ergebnisse für Ihr Konto.

Nachdem Sie sich vom Administratorkonto getrennt haben, bleibt die Einladung, Mitglied zu werden, weiterhin bestehen. Sie können die Einladung in future erneut annehmen.

Security Hub console

Um die Verbindung zu Ihrem Administratorkonto zu trennen

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Einstellungen und dann Konten aus.
3. Deaktivieren Sie im Abschnitt Administratorkonto die Option Annehmen und wählen Sie dann Aktualisieren aus.

Security Hub API

Um die Verbindung zu Ihrem Administratorkonto zu trennen

Rufen Sie die API auf `DisassociateFromAdministratorAccount`.

AWS CLI

Um die Verbindung zu Ihrem Administratorkonto zu trennen

Führen Sie den Befehl `disassociate-from-administrator-account` aus.

```
aws securityhub disassociate-from-administrator-account
```

> **Note**
>
> Die Security Hub Hub-Konsole wird weiterhin verwendet`DisassociateFromMasterAccount`. Sie wird irgendwann auf Verwendung umgestellt`DisassociateFromAdministratorAccount`. Alle IAM-Richtlinien, die speziell den Zugriff auf diese Funktion steuern, müssen weiterhin verwendet `DisassociateFromMasterAccount` werden. Sie sollten Ihre Richtlinien auch ergänzen`DisassociateFromAdministratorAccount`, um sicherzustellen, dass nach

Beginn der Nutzung `DisassociateFromAdministratorAccount` der Konsole die richtigen Berechtigungen vorhanden sind.

Umstellung auf die AWS Organizations Kontoverwaltung

Wenn Sie Konten manuell verwaltenAWS Security Hub, müssen Sie potenzielle Mitgliedskonten einladen und jedes Mitgliedskonto in jedem Konto separat konfigurierenAWS-Region.

Durch die Integration von Security Hub und AWS Organizations können Sie das Senden von Einladungen überflüssig machen und mehr Kontrolle darüber gewinnen, wie Security Hub in Ihrem Unternehmen konfiguriert und angepasst wird.

Es ist möglich, einen kombinierten Ansatz zu verwenden, bei dem Sie die AWS Organizations Integration verwenden, aber auch Konten außerhalb Ihrer Organisation manuell einladen. Wir empfehlen jedoch, ausschließlich die Organizations-Integration zu verwenden. Die zentrale Konfiguration, eine Funktion, mit der Sie Security Hub über mehrere Konten und Regionen hinweg verwalten können, ist nur verfügbar, wenn Sie es mit Organizations integrieren.

In diesem Abschnitt wird beschrieben, wie Sie von der manuellen Kontoverwaltung auf Einladungsbasis zur Verwaltung von Konten mit übergehen können. AWS Organizations

Integration von Security Hub mit AWS Organizations

Zunächst müssen Sie Security Hub und integrierenAWS Organizations.

Sie können diese Dienste integrieren, indem Sie die folgenden Schritte ausführen:

- Erstellen Sie eine Organisation inAWS Organizations. Anweisungen finden Sie im AWS OrganizationsBenutzerhandbuch unter Organisation erstellen.
- Geben Sie im Verwaltungskonto Organizations ein delegiertes Security Hub-Administratorkonto an.

> **Note**
>
> Das Verwaltungskonto der Organisation kann nicht als DA-Konto festgelegt werden.

Detaillierte Anweisungen finden Sie unter Integrieren von Security Hub mit AWS Organizations.

Indem Sie die vorherigen Schritte ausführen, gewähren Sie vertrauenswürdigen Zugriff für Security Hub inAWS Organizations. Dadurch wird Security Hub auch im aktuellen Administratorkonto AWS-Region für das delegierte Administratorkonto aktiviert.

Der delegierte Administrator kann die Organisation in Security Hub verwalten, indem er in erster Linie die Konten der Organisation als Security Hub Hub-Mitgliedskonten hinzufügt. Der Administrator kann auch auf bestimmte Security Hub Hub-Einstellungen, Daten und Ressourcen für diese Konten zugreifen.

Wenn Sie mit Organizations zur Kontoverwaltung wechseln, werden Konten, die auf Einladung basieren, nicht automatisch zu Security Hub Hub-Mitgliedern. Nur die Konten, die Sie zu Ihrer neuen Organisation hinzufügen, können Security Hub Hub-Mitglieder werden.

Zentrale Konfiguration im Vergleich zu lokaler Konfiguration

Nach der Aktivierung der Integration können Sie Konten bei Organizations verwalten. Weitere Informationen finden Sie unter Konten verwalten mit AWS Organizations. Die Kontoverwaltung variiert je nach Konfigurationstyp Ihrer Organisation.

Es gibt zwei mögliche Konfigurationstypen für Ihre Organisation: lokal und zentral. Ihr Standardkonfigurationstyp ist lokale Konfiguration. Um Ihren aktuellen Konfigurationstyp zu sehen, wählen Sie im Navigationsbereich der Security Hub Hub-Konsole Einstellungen und dann Konfiguration. Sie können auch die `DescribeOrganizationConfiguration`API aufrufen, um Ihren Konfigurationstyp anzuzeigen.

In der lokalen Konfiguration kann das delegierte Administratorkonto festlegen, dass Security Hub und Standardsicherheitsstandards für neue Konten automatisch aktiviert werden, wenn diese der Organisation beitreten. Diese neuen Kontoeinstellungen werden in der aktuellen Region wirksam. Andere Security Hub Hub-Einstellungen müssen für jedes Mitgliedskonto in jeder Region separat konfiguriert werden.

Wir empfehlen, die zentrale Konfiguration statt der lokalen Konfiguration zu verwenden.
Bei der zentralen Konfiguration kann das delegierte Administratorkonto Security Hub Hub-Konfigurationsrichtlinien erstellen, die für mehrere Regionen gelten und die Security Hub Hub-Funktionen in den verschiedenen Konten und Organisationseinheiten (OUs) Ihres Unternehmens spezifizieren. Sie können eine einzige Konfigurationsrichtlinie auf Ihre gesamte Organisation oder unterschiedliche Konfigurationsrichtlinien auf verschiedene Konten und Organisationseinheiten anwenden. Sie können beispielsweise einen Satz von Standards und Kontrollen in Produktionskonten und einen anderen Satz von Standards und Kontrollen in Testkonten aktivieren. Der DA kann die Konfigurationsrichtlinien nach Bedarf bearbeiten.

Weitere Informationen zur Funktionsweise der zentralen Konfiguration finden Sie unterSo funktioniert die zentrale Konfiguration.

Anweisungen zum Umschalten von der lokalen zur zentralen Konfiguration finden Sie unterBeginnen Sie mit der zentralen Konfiguration.

Zulässige Aktionen für Konten

Administrator- und Mitgliedskonten haben Zugriff auf die in den folgenden Tabellen aufgeführten AWS Security Hub Aktionen. In den Tabellen haben die Werte die folgenden Bedeutungen:

- Beliebig — Das Konto kann die Aktion für jedes Mitgliedskonto unter demselben Administrator ausführen.
- Aktuell — Das Konto kann die Aktion nur für sich selbst ausführen (das Konto, bei dem Sie derzeit angemeldet sind).
- Dash — Zeigt an, dass das Konto die Aktion nicht ausführen kann.

Wie in den Tabellen angegeben, hängen die zulässigen Aktionen davon ab, ob Sie eine Integration vornehmen AWS Organizations und welchen Konfigurationstyp Ihre Organisation verwendet. Informationen zum Unterschied zwischen zentraler und lokaler Konfiguration finden Sie unterVerwalten von Konten mit AWS Organizations.

Security Hub kopiert die Ergebnisse des Mitgliedskontos nicht in das Administratorkonto. In Security Hub werden alle Ergebnisse für ein bestimmtes Konto in einer bestimmten Region erfasst. In jeder Region kann das Administratorkonto die Ergebnisse für seine Mitgliedskonten in dieser Region einsehen und verwalten.

Wenn Sie eine Aggregationsregion festlegen, kann das Administratorkonto die Ergebnisse von Mitgliedskonten aus verknüpften Regionen anzeigen und verwalten, die in die Aggregationsregion repliziert werden. Weitere Informationen zur regionsübergreifenden Aggregation finden Sie unter Regionsübergreifende Aggregation.

Diese Tabelle enthält die Standardberechtigungen für Administrator- und Mitgliedskonten. Sie können benutzerdefinierte IAM-Richtlinien verwenden, um den Zugriff auf die Features und Funktionen von Security Hub weiter einzuschränken. Anleitungen und Beispiele finden Sie im Blogbeitrag Aligning IAM-Policies to user personas for. AWS Security Hub

Zulässige Aktionen, wenn Sie in Organizations integrieren und die zentrale Konfiguration verwenden

Administrator- und Mitgliedskonten können wie folgt auf Security Hub Hub-Aktionen zugreifen, wenn Sie Organizations integrieren und die zentrale Konfiguration verwenden.

Action	Delegiertes Security Hub-Administratorkonto	Zentral verwaltetes Mitgliedskonto	Selbstverwaltetes Mitgliedskonto
Security Hub Hub-Konfigurationsrichtlinien erstellen und verwalten	Für selbst und zentral verwaltete Konten	–	–
Organisationskonten anzeigen	Any	–	–
Mitgliedskonto trennen	Any	–	–
Mitgliedskonto löschen	Jedes Konto, das nicht zur Organisation gehört	–	–
Security Hub deaktivieren	Für Girokonten und zentral verwaltete Konten	–	Aktuell
Ergebnisse und Fundverlauf anzeigen	Any	Aktuell	Aktuell
Ergebnisse aktualisieren	Any	Aktuell	Aktuell
Insight-Ergebnisse anzeigen	Any	Aktuell	Aktuell

Action	Delegiertes Security Hub-Administratorkonto	Zentral verwaltetes Mitgliedskonto	Selbstverwaltetes Mitgliedskonto
Kontrolldetails anzeigen	Any	Aktuell	Aktuell
Schalten Sie konsolidierte Kontrollergebnisse ein oder aus	Any	–	–
Aktivieren und deaktivieren Sie Standards	Für Girokonten und zentral verwaltete Konten	–	Aktuell
Steuerungen aktivieren und deaktivieren	Für Girokonten und zentral verwaltete Konten	–	Aktuell
Integrationen aktivieren und deaktivieren	Aktuell	Aktuell	Aktuell
Konfigurieren Sie die regionsübergreifende Aggregation	Any	–	–
Wählen Sie die Heimatregion und die verknüpften Regionen aus	Beliebig (Sie müssen die zentrale Konfiguration beenden und neu starten, um die Heimatregion zu ändern)	–	–
Konfigurieren Sie benutzerdefinierte Aktionen	Aktuell	Aktuell	Aktuell

Action	Delegiertes Security Hub-Administratorkonto	Zentral verwaltetes Mitgliedskonto	Selbstverwaltetes Mitgliedskonto
Konfigurieren Sie Automatisierungsregeln	Any	–	–
Konfigurieren Sie benutzerdefinierte Einblicke	Aktuell	Aktuell	Aktuell

Zulässige Aktionen, wenn Sie eine Integration mit Organizations durchführen und die lokale Konfiguration verwenden

Administrator- und Mitgliedskonten können wie folgt auf Security Hub Hub-Aktionen zugreifen, wenn Sie Organizations integrieren und die lokale Konfiguration verwenden.

Action	Delegiertes Security Hub-Administratorkonto	Mitgliedskonto
Security Hub Hub-Konfigurationsrichtlinien erstellen und verwalten	–	–
Organisationskonten anzeigen	Any	–
Mitgliedskonto trennen	Any	–
Mitgliedskonto löschen	–	–
Security Hub deaktivieren	–	Aktuell (wenn das Konto vom delegierten Administrator getrennt ist)
Ergebnisse und Fundverlauf anzeigen	Any	Aktuell

Action	Delegiertes Security Hub-Administratorkonto	Mitgliedskonto
Ergebnisse aktualisieren	Any	Aktuell
Insight-Ergebnisse anzeigen	Any	Aktuell
Kontrolldetails anzeigen	Any	Aktuell
Schalten Sie konsolidierte Kontrollergebnisse ein oder aus	Any	–
Aktivieren und deaktivieren Sie Standards	Aktuell	Aktuell
Automatisches Aktivieren von Security Hub und Standards tandards in neuen Unternehm enskonten	Für Girokonten und neue Unternehmenskonten	–
Steuerelemente aktivieren und deaktivieren	Aktuell	Aktuell
Integrationen aktivieren und deaktivieren	Aktuell	Aktuell
Konfigurieren Sie die regionsübergreifende Aggregation	Any	–
Konfigurieren Sie benutzerd efinierte Aktionen	Aktuell	Aktuell
Konfigurieren Sie Automatis ierungsregeln	Any	–
Konfigurieren Sie benutzerd efinierte Einblicke	Aktuell	Aktuell

Zulässige Aktionen für Konten, die auf Einladungen basieren

Administrator- und Mitgliedskonten können wie folgt auf Security Hub Hub-Aktionen zugreifen, wenn Sie die auf Einladung basierende Methode verwenden, um Konten manuell zu verwalten, anstatt sie zu integrieren. AWS Organizations

Action	Security Hub-Administratorkonto	Mitgliedskonto
Security Hub Hub-Konfigurationsrichtlinien erstellen und verwalten	–	–
Organisationskonten anzeigen	Any	–
Mitgliedskonto trennen	Any	Aktuell
Mitgliedskonto löschen	Any	–
Security Hub deaktivieren	Aktuell (falls keine aktivierten Mitgliedskonten vorhanden sind)	Aktuell (wenn das Konto vom Administratorkonto getrennt ist)
Ergebnisse und Fundverlauf anzeigen	Any	Aktuell
Ergebnisse aktualisieren	Any	Aktuell
Insight-Ergebnisse anzeigen	Any	Aktuell
Kontrolldetails anzeigen	Any	Aktuell
Schalten Sie konsolidierte Kontrollergebnisse ein oder aus	Any	–
Aktivieren und deaktivieren Sie Standards	Aktuell	Aktuell

Action	Security Hub-Administratorkonto	Mitgliedskonto
Automatisches Aktivieren von Security Hub und Standards tandards in neuen Unternehmenskonten	–	–
Steuerungen aktivieren und deaktivieren	Aktuell	Aktuell
Integrationen aktivieren und deaktivieren	Aktuell	Aktuell
Konfigurieren Sie die regionsübergreifende Aggregation	Any	–
Konfigurieren Sie benutzerdefinierte Aktionen	Aktuell	Aktuell
Konfigurieren Sie Automatisierungsregeln	Any	–
Konfigurieren Sie benutzerdefinierte Einblicke	Aktuell	Aktuell

Einschränkungen und Empfehlungen für die Kontoverwaltung

Im folgenden Abschnitt werden einige Einschränkungen und Empfehlungen zusammengefasst, die Sie bei der Verwaltung von Mitgliedskonten in beachten sollten AWS Security Hub.

Maximale Anzahl von Mitgliedern pro Konto

Wenn Sie die Integration mit verwenden AWS Organizations, unterstützt Security Hub bis zu 10 000 Mitgliedskonten pro delegiertem Administratorkonto in jeder AWS-Region. Wenn Sie Security Hub manuell aktivieren und verwalten, unterstützt Security Hub bis zu 1 000 Mitgliedskontoeinladungen pro Administratorkonto in jeder Region.

Konten und Regionen

Mitgliedschaft nach Organisation

Wenn Sie Security Hub in integrieren AWS Organizations, kann das Organizations-Verwaltungskonto ein delegiertes Administratorkonto (DA) für Security Hub festlegen. Das Verwaltungskonto der Organisation kann in Organizations nicht als DA festgelegt werden. Obwohl dies in Security Hub zulässig ist, empfehlen wir, dass das Verwaltungskonto von Organizations nicht die DA sein sollte.

Wir empfehlen Ihnen, dasselbe DA-Konto in allen Regionen auszuwählen. Wenn Sie die zentrale Konfiguration verwenden, legt Security Hub dasselbe DA-Konto in allen Regionen fest, in denen Sie Security Hub für Ihre Organisation konfigurieren.

Wir empfehlen Ihnen auch, dasselbe DA-Konto für AWS Sicherheits- und Compliance-Services zu wählen, um Sie bei der Verwaltung sicherheitsrelevanter Probleme in einem einzigen Bereich zu unterstützen.

Mitgliedschaft auf Einladung

Bei Mitgliedskonten, die auf Einladung erstellt wurden, wird die Kontozuordnung des Administratormitglieds nur in der Region erstellt, aus der die Einladung gesendet wird. Das Administratorkonto muss Security Hub in jeder Region aktivieren, in der Sie es verwenden möchten. Das Administratorkonto lädt dann jedes Konto ein, ein Mitgliedskonto in dieser Region zu werden.

Einschränkungen für Beziehungen zwischen Administratoren und Mitgliedern

> **Note**
>
> Wenn Sie die Security Hub-Integration mit verwenden AWS Organizationsund keine Mitgliedskonten manuell eingeladen haben, gilt dieser Abschnitt nicht für Sie.

Ein -Konto darf nicht gleichzeitig ein Administratorkonto und ein Mitgliedskonto sein.

Ein Mitgliedskonto kann nur einem Administratorkonto zugeordnet werden. Wenn ein Organisationskonto durch das Security Hub-Administratorkonto aktiviert wird, kann das Konto keine Einladung von einem anderen Konto annehmen. Wenn ein Konto bereits eine Einladung

angenommen hat, kann das Konto nicht über das Security Hub-Administratorkonto für die Organisation aktiviert werden. Es kann auch keine Einladungen von anderen Konten erhalten.

Für den manuellen Einladungsprozess ist die Annahme einer Mitgliedschaftseinladung optional.

Koordination von Administratorkonten über -Services hinweg

Security Hub aggregiert Erkenntnisse aus verschiedenen - AWS Services, wie Amazon GuardDuty, Amazon Inspector und Amazon Macie . Security Hub ermöglicht es Benutzern auch, von einer GuardDuty Erkenntnis zu wechseln, um eine Untersuchung in Amazon Detective zu starten.

Die Beziehungen zwischen Administratoren und Mitgliedern, die Sie in diesen anderen Services eingerichtet haben, gelten jedoch nicht automatisch für Security Hub. Security Hub empfiehlt Ihnen, dasselbe Konto wie das Administratorkonto für alle diese Services zu verwenden. Dieses Administratorkonto sollte ein Konto sein, das für Sicherheitstools verantwortlich ist. Dasselbe Konto sollte auch das Aggregatorkonto für sein AWS Config.

Beispielsweise kann ein Benutzer aus dem GuardDuty Administratorkonto A Ergebnisse für GuardDuty die Mitgliedskonten B und C in der - GuardDuty Konsole sehen. Wenn Konto A Security Hub aktiviert, sehen GuardDuty Benutzer aus Konto A nicht automatisch Ergebnisse für die Konten B und C in Security Hub. Für diese Konten ist auch eine Security Hub-Administratormitgliedsbeziehung erforderlich.

Dazu machen Sie Konto A zum Security Hub-Administratorkonto und ermöglichen Sie den Konten B und C, Security Hub-Mitgliedskonten zu werden.

Auswirkung von Kontoaktionen auf Security Hub Hub-Daten

Diese Kontoaktionen haben die folgenden Auswirkungen auf AWS Security Hub Daten.

Security Hub deaktiviert

Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte Administrator (DA) Security Hub Hub-Konfigurationsrichtlinien erstellen, die AWS Security Hub in bestimmten Konten und Organisationseinheiten (OUs) deaktiviert werden. In diesem Fall ist Security Hub in den angegebenen Konten und Organisationseinheiten in Ihrer Heimatregion und allen verknüpften Regionen deaktiviert.

Wenn Sie die zentrale Konfiguration nicht verwenden, müssen Sie Security Hub für jedes Konto und jede Region, in der Sie ihn aktiviert haben, separat deaktivieren.

Für das Administratorkonto werden keine neuen Ergebnisse generiert, wenn Security Hub im Administratorkonto deaktiviert ist. Sie können die zentrale Konfiguration auch nicht verwenden, wenn Security Hub im DA-Konto deaktiviert ist. Vorhandene Erkenntnisse werden nach 90 Tagen gelöscht.

Integrationen mit anderen AWS-Services werden entfernt.

Aktivierte Sicherheitsstandards und Kontrollen sind deaktiviert.

Andere Security Hub Hub-Daten und -Einstellungen, einschließlich benutzerdefinierter Aktionen, Einblicke und Abonnements für Produkte von Drittanbietern, werden beibehalten.

Das Mitgliedskonto wurde vom Administratorkonto getrennt

Wenn ein Mitgliedskonto vom Administratorkonto getrennt wird, verliert das Administratorkonto die Berechtigung, Ergebnisse im Mitgliedskonto einzusehen. Security Hub ist jedoch weiterhin in beiden Konten aktiviert.

Wenn Sie die zentrale Konfiguration verwenden, kann der DA Security Hub nicht für ein Mitgliedskonto konfigurieren, das vom DA-Konto getrennt ist.

Benutzerdefinierte Einstellungen oder Integrationen, die für das Administratorkonto definiert sind, werden nicht auf Ergebnisse aus dem früheren Mitgliedskonto angewendet. Wenn die Konten beispielsweise getrennt wurden, haben Sie möglicherweise eine benutzerdefinierte Aktion im Administratorkonto, die als Ereignismuster in einer EventBridge Amazon-Regel verwendet wird. Diese benutzerdefinierte Aktion kann jedoch nicht im Mitgliedskonto verwendet werden.

In der Kontenliste für das Security Hub-Administratorkonto hat ein entferntes Konto den Status Getrennt.

Das Mitgliedskonto wurde aus einer Organisation entfernt

Wenn ein Mitgliedskonto aus einer Organisation entfernt wird, verliert das Security Hub-Administratorkonto die Berechtigung, Ergebnisse im Mitgliedskonto einzusehen. Security Hub ist jedoch weiterhin in beiden Konten mit denselben Einstellungen aktiviert, die sie vor dem Entfernen hatten.

Wenn Sie die zentrale Konfiguration verwenden, können Sie Security Hub nicht für ein Mitgliedskonto konfigurieren, nachdem es aus der Organisation entfernt wurde, zu der der delegierte Administrator gehört. Das Konto behält jedoch die Einstellungen bei, die es vor der Entfernung hatte, sofern Sie sie nicht manuell ändern.

In der Kontenliste für das Security Hub-Administratorkonto hat ein entferntes Konto den Status Gelöscht.

Das Konto ist gesperrt

Wenn ein Konto gesperrt wirdAWS, verliert das Konto die Erlaubnis, seine Ergebnisse im Security Hub einzusehen. Für dieses Konto werden keine neuen Ergebnisse generiert. Das Administratorkonto für ein gesperrtes Konto kann die Ergebnisse des bestehenden Kontos einsehen.

Bei einem Unternehmenskonto kann der Status des Mitgliedskontos auch in Konto gesperrt geändert werden. Dies ist der Fall, wenn das Konto gleichzeitig gesperrt wird, während das Administratorkonto versucht, das Konto zu aktivieren. Das Administratorkonto für ein gesperrtes Konto kann die Ergebnisse für dieses Konto nicht einsehen. Andernfalls hat der Status „Gesperrt“ keinen Einfluss auf den Status des Mitgliedskontos.

Wenn Sie die zentrale Konfiguration verwenden, schlägt die Richtlinienzuweisung fehl, wenn der delegierte Administrator versucht, einem gesperrten Konto eine Konfigurationsrichtlinie zuzuordnen.

Nach 90 Tagen wird das Konto entweder gekündigt oder reaktiviert. Wenn das Konto reaktiviert wird, werden seine Security Hub Hub-Berechtigungen wiederhergestellt. Wenn das Mitgliedskonto den Status Konto gesperrt hat, muss das Administratorkonto das Konto manuell aktivieren.

Das Konto ist geschlossen

Wenn ein geschlossen AWS-Konto wird, reagiert Security Hub wie folgt auf das Schließen.

Security Hub bewahrt die Ergebnisse für das Konto für einen Zeitraum von 90 Tagen ab dem Datum des Inkrafttretens der Kontoschließung auf. Am Ende des 90-Tage-Zeitraums löscht Security Hub dauerhaft alle Ergebnisse für das Konto.

- Um Ergebnisse länger als 90 Tage aufzubewahren, können Sie eine benutzerdefinierte Aktion mit einer EventBridge Regel verwenden, um die Ergebnisse in einem Amazon S3 S3-Bucket zu speichern. Solange Security Hub die Ergebnisse aufbewahrt, stellt Security Hub die Ergebnisse für das Konto wieder her, wenn Sie das geschlossene Konto erneut öffnen.
- Wenn es sich bei dem Konto um ein Security Hub-Administratorkonto handelt, wird es als Administrator entfernt und alle Mitgliedskonten werden entfernt. Wenn es sich bei dem Konto um ein Mitgliedskonto handelt, wird es getrennt und als Mitglied aus dem Security Hub-Administratorkonto entfernt.

- Weitere Informationen finden Sie unter Schließen eines Kontos im AWSBilling and Cost Management-Benutzerhandbuch.

> **Important**
>
> Für Kunden in den AWS GovCloud (US)-Regionen:
>
> - Sichern Sie vor dem Schließen Ihres Kontos die Richtliniendaten und löschen Sie dann zusammen mit anderen Kontoressourcen. Nach dem Schließen des Kontos haben Sie keinen Zugriff mehr darauf.

Regionsübergreifende Aggregation

Mit der regionsübergreifenden Aggregation können Sie Ergebnisse zusammenfassen, Aktualisierungen und Erkenntnisse finden, den Compliance-Status und Sicherheitswerte aus mehreren Regionen in einer einzigen Aggregationsregion kontrollieren. Anschließend können Sie all diese Daten aus der Aggregationsregion verwalten.

> **Note**
>
> In AWS GovCloud (US) wird die regionsübergreifende Aggregation nur für Ergebnisse, Suchaktualisierungen und Erkenntnisse in allen Bereichen unterstützt. AWS GovCloud (US) Insbesondere können Sie nur Ergebnisse, Aktualisierungen und Erkenntnisse zwischen AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) zusammenfassen. In den Regionen Chinas wird die regionsübergreifende Aggregation nur für Ergebnisse, Aktualisierungen und Erkenntnisse aus allen Regionen Chinas unterstützt. Insbesondere können Sie Ergebnisse, Aktualisierungen und Erkenntnisse nur zwischen China (Peking) und China (Ningxia) zusammenfassen.

Angenommen, Sie haben USA Ost (Nord-Virginia) als Aggregationsregion und USA West (Oregon) und USA West (Nordkalifornien) als Ihre verknüpften Regionen festgelegt. Wenn Sie die Ergebnisseite in USA Ost (Nord-Virginia) aufrufen, sehen Sie die Ergebnisse aus allen drei Regionen. Aktualisierungen dieser Ergebnisse spiegeln sich auch in allen drei Regionen wider.

Der Aktivierungsstatus einer Steuerung muss in jeder Region geändert werden. Wenn ein Steuerelement in einer verknüpften Region aktiviert, aber in der Aggregationsregion deaktiviert ist, können Sie den Konformitätsstatus des Steuerelements in der Aggregationsregion anzeigen, aber Sie können dieses Steuerelement nicht in der Aggregationsregion aktivieren oder deaktivieren.

Um regionsübergreifende Sicherheitsbewertungen und Compliance-Status anzuzeigen, fügen Sie Ihrer IAM-Rolle, die Security Hub verwendet, die folgenden Berechtigungen hinzu:

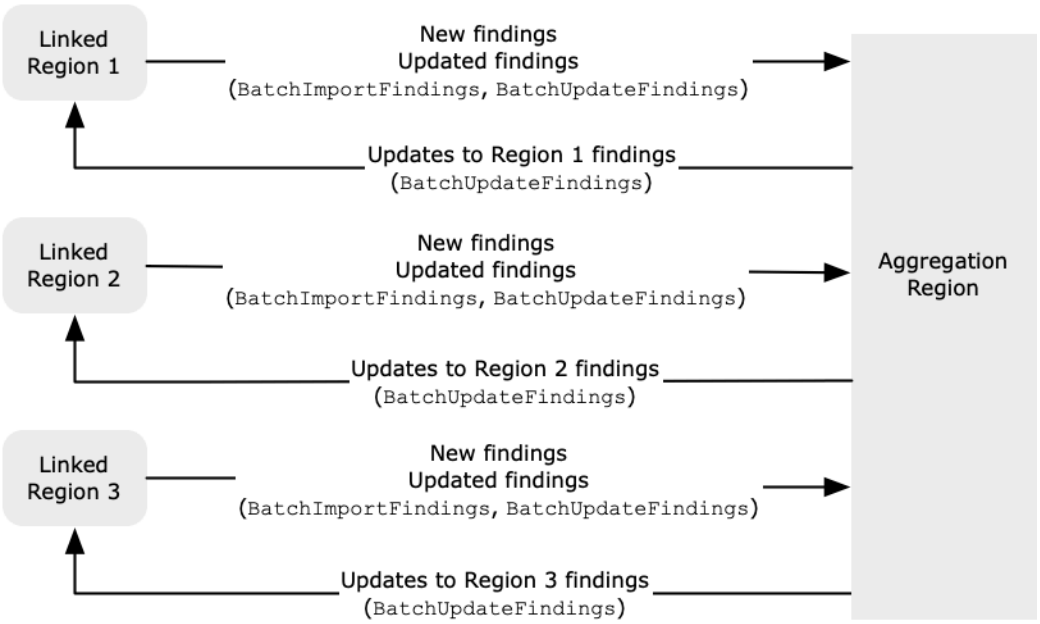
- `ListSecurityControlDefinitions`
- `BatchGetStandardsControlAssociations`
- `BatchUpdateStandardsControlAssociations`

So funktioniert die regionsübergreifende Aggregation

Wenn die regionsübergreifende Aggregation aktiviert ist, repliziert Security Hub die folgenden Daten aus den verknüpften Regionen in die Aggregationsregion. Dies geschieht in jedem Konto, für das die regionsübergreifende Aggregation aktiviert ist.

- Funde
- Insights
- Kontrollieren Sie den Compliance-Status
- Sicherheitswerte

Zusätzlich zu den neuen Daten in der vorherigen Liste repliziert Security Hub auch Aktualisierungen dieser Daten zwischen den verknüpften Regionen und der Aggregationsregion. Aktualisierungen, die in einer verknüpften Region auftreten, werden in die Aggregationsregion repliziert. Aktualisierungen, die in der Aggregationsregion vorgenommen werden, werden zurück in die verknüpfte Region repliziert.



Wenn es in der Aggregationsregion und der verknüpften Region widersprüchliche Aktualisierungen gibt, wird die neueste Aktualisierung verwendet.

Die regionsübergreifende Aggregation erhöht die Kosten von Security Hub nicht. Es fallen keine Gebühren an, wenn Security Hub neue Daten oder Updates repliziert.

In der Aggregationsregion bietet die Übersichtsseite einen Überblick über Ihre aktiven Ergebnisse in den verknüpften Regionen. Weitere Informationen finden Sie unter Eine regionsübergreifende Zusammenfassung der Ergebnisse nach Schweregrad anzeigen. In anderen Bereichen auf der Übersichtsseite, in denen Ergebnisse analysiert werden, werden ebenfalls Informationen aus allen verknüpften Regionen angezeigt.

Ihre Sicherheitswerte in der Aggregationsregion werden berechnet, indem die Anzahl der bestandenen Kontrollen mit der Anzahl der aktivierten Kontrollen in allen verknüpften Regionen verglichen wird. Wenn ein Steuerelement in mindestens einer verknüpften Region aktiviert ist, ist es außerdem auf den Detailseiten mit den Sicherheitsstandards der Aggregationsregion sichtbar. Der Konformitätsstatus der Kontrollen auf den Seiten mit den Standarddetails spiegelt die Ergebnisse der verknüpften Regionen wider. Wenn eine mit einer Kontrolle verknüpfte Sicherheitsüberprüfung in einer oder mehreren verknüpften Regionen fehlschlägt, wird der Konformitätsstatus dieser Kontrolle auf den Standarddetailseiten der Aggregationsregion als Fehlgeschlagen angezeigt. Die Anzahl der Sicherheitsprüfungen umfasst Ergebnisse aus allen verknüpften Regionen.

Security Hub aggregiert nur Daten aus Regionen, in denen Security Hub für ein Konto aktiviert ist. Security Hub wird nicht automatisch für ein Konto aktiviert, das auf der regionsübergreifenden Aggregationskonfiguration basiert.

Aggregation für Administrator- und Mitgliedskonten

Eigenständige Konten, Mitgliedskonten und Administratorkonten können die regionsübergreifende Aggregation konfigurieren. Falls von einem Administrator konfiguriert, ist das Vorhandensein des Administratorkontos unerlässlich, damit die regionsübergreifende Aggregation in verwalteten Konten funktioniert. Wenn das Administratorkonto entfernt oder von einem Mitgliedskonto getrennt wird, wird die regionsübergreifende Aggregation für das Mitgliedskonto beendet. Dies gilt auch dann, wenn für das Konto die regionsübergreifende Aggregation aktiviert war, bevor die Beziehung zwischen Administrator und Mitglied aufgenommen wurde.

Wenn ein Administratorkonto die regionsübergreifende Aggregation aktiviert, repliziert Security Hub die Daten, die das Administratorkonto in allen verknüpften Regionen generiert, in die Aggregationsregion. Darüber hinaus identifiziert Security Hub die Mitgliedskonten, die diesem Administrator zugeordnet sind, und jedes Mitgliedskonto erbt die regionsübergreifenden Aggregationseinstellungen des Administrators. Security Hub repliziert die Daten, die ein Mitgliedskonto in allen verknüpften Regionen generiert, in die Aggregationsregion.

Der Administrator kann von allen Mitgliedskonten in den verwalteten Regionen aus auf Sicherheitsergebnisse zugreifen und diese verwalten. Als Security Hub-Administrator müssen Sie

jedoch in der Aggregationsregion angemeldet sein, um aggregierte Daten aus allen Mitgliedskonten und verknüpften Regionen anzeigen zu können.

Als Security Hub-Mitgliedskonto müssen Sie in der Aggregationsregion angemeldet sein, um aggregierte Daten aus Ihrem Konto aus allen verknüpften Regionen anzeigen zu können. Mitgliedskonten sind nicht berechtigt, Daten von anderen Mitgliedskonten einzusehen.

Ein Administratorkonto kann Mitgliedskonten manuell einladen oder als delegierter Administrator einer Organisation fungieren, in die integriert AWS Organizations ist. Bei einem Mitgliedskonto mit manueller Einladung muss der Administrator das Konto aus der Aggregationsregion und allen verknüpften Regionen einladen, damit die regionsübergreifende Aggregation funktioniert. Darüber hinaus muss Security Hub für das Mitgliedskonto in der Aggregationsregion und allen verknüpften Regionen aktiviert sein, damit der Administrator die Ergebnisse des Mitgliedskontos einsehen kann. Wenn Sie die Aggregationsregion nicht für andere Zwecke verwenden, können Sie die Security Hub Hub-Standards und -Integrationen in dieser Region deaktivieren, um Gebühren zu vermeiden.

Wenn Sie die regionsübergreifende Aggregation verwenden möchten und über mehrere Administratorkonten verfügen, empfehlen wir Ihnen, die folgenden bewährten Methoden zu befolgen:

- Jedes Administratorkonto hat unterschiedliche Mitgliedskonten.
- Jedes Administratorkonto hat in allen Regionen dieselben Mitgliedskonten.
- Jedes Administratorkonto verwendet eine andere Aggregationsregion.

> **Note**
>
> Informationen darüber, wie sich die regionsübergreifende Aggregation auf die zentrale Konfiguration auswirkt, finden Sie unter. Zentrale Konfiguration und regionsübergreifende Aggregation

Zentrale Konfiguration und regionsübergreifende Aggregation

Die zentrale Konfiguration ist eine optionale Funktion in Security Hub, die Sie verwenden können, wenn Sie sie integrieren AWS Organizations. Wenn Sie die zentrale Konfiguration verwenden, kann das delegierte Administratorkonto den Security Hub Hub-Dienst, die Standards und Kontrollen für Konten und Organisationseinheiten (OU) in der Organisation konfigurieren. Um Konten und Organisationseinheiten zu konfigurieren, erstellt der delegierte Administrator Security Hub Hub-

Konfigurationsrichtlinien. Mithilfe von Konfigurationsrichtlinien kann definiert werden, ob Security Hub aktiviert oder deaktiviert ist und welche Standards und Kontrollen aktiviert sind. Der delegierte Administrator ordnet Konfigurationsrichtlinien bestimmten Konten, Organisationseinheiten oder dem Stamm (der gesamten Organisation) zu.

Der delegierte Administrator kann Konfigurationsrichtlinien für die Organisation nur in der Aggregationsregion erstellen und verwalten. Darüber hinaus werden Konfigurationsrichtlinien in der Aggregationsregion und allen verknüpften Regionen wirksam. Sie können keine Konfigurationsrichtlinie erstellen, die nur für einige verknüpfte Regionen gilt und nicht für andere. In der zentralen Konfiguration wird die Aggregationsregion als Heimatregion bezeichnet. Dieselbe Region muss für die Zwecke der zentralen Konfiguration als Heimatregion und für die Zwecke der regionsübergreifenden Aggregation als Aggregationsregion dienen. Informationen zur regionsübergreifenden Aggregation finden Sie unter Regionsübergreifende Aggregation.

Um die zentrale Konfiguration zu verwenden, müssen Sie eine Heimatregion und mindestens eine verknüpfte Region angeben.

Eine Änderung Ihrer regionsübergreifenden Aggregationseinstellungen kann sich auf Ihre Konfigurationsrichtlinien auswirken. Wenn Sie eine verknüpfte Region hinzufügen, werden Ihre Konfigurationsrichtlinien in dieser Region wirksam. Wenn es sich bei der Region um eine Opt-in-Region handelt, muss die Region aktiviert sein, damit Ihre Konfigurationsrichtlinien dort wirksam werden. Umgekehrt sind die Konfigurationsrichtlinien in dieser Region nicht mehr wirksam, wenn Sie eine verknüpfte Region entfernen. In dieser Region behalten die Konten die Einstellungen bei, die sie hatten, als die verknüpfte Region entfernt wurde. Sie können diese Einstellungen ändern, müssen dies jedoch für jedes Konto und jede Region separat tun.

Wenn Sie die Heimatregion entfernen oder ändern, werden Ihre Konfigurationsrichtlinien und Richtlinienverknüpfungen gelöscht. Sie können in keiner Region mehr die zentrale Konfiguration verwenden oder Konfigurationsrichtlinien erstellen. Konten behalten die Einstellungen bei, die sie hatten, bevor die Heimatregion geändert oder entfernt wurde. Sie können diese Einstellungen jederzeit ändern. Da Sie die zentrale Konfiguration jedoch nicht mehr verwenden, müssen die Einstellungen für jedes Konto und jede Region separat geändert werden. Sie können die zentrale Konfiguration verwenden und erneut Konfigurationsrichtlinien erstellen, wenn Sie eine neue Heimatregion angeben.

Weitere Informationen zur zentralen Konfiguration finden Sie unterSo funktioniert die zentrale Konfiguration.

Aktivierung der regionsübergreifenden Aggregation

Sie müssen die regionsübergreifende Aggregation von der Region aus aktivieren AWS-Region , die Sie als Aggregationsregion festlegen möchten.

Sie können eine Region, die standardmäßig deaktiviert ist, nicht als Ihre Aggregationsregion verwenden. Eine Liste der Regionen, die standardmäßig deaktiviert sind, finden Sie unter Aktivieren einer Region in der Allgemeine AWS-Referenz.

Aktivierung der regionsübergreifenden Aggregation (Konsole)

Wenn Sie die regionsübergreifende Aggregation aktivieren, wählen Sie Ihre verknüpften Regionen aus. Sie entscheiden auch, ob neue Regionen automatisch verknüpft werden sollen, wenn Security Hub beginnt, sie zu unterstützen und Sie sich für sie entschieden haben.

Um die regionsübergreifende Aggregation zu aktivieren

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Melden Sie sich mit dem AWS-Region Selektor bei der Region an, die Sie als Aggregationsregion verwenden möchten.
3. Wählen Sie im Security Hub-Navigationsmenü Einstellungen und dann Regionen.
4. Wählen Sie unter Suchaggregation die Option Suchaggregation konfigurieren aus.

   Standardmäßig ist die Aggregationsregion auf Keine Aggregationsregion gesetzt.
5. Wählen Sie unter Aggregationsregion die Option aus, um die aktuelle Region als Aggregationsregion festzulegen.
6. Wählen Sie optional für Verknüpfte Regionen die Regionen aus, aus denen Daten aggregiert werden sollen.
7. Um Daten aus neuen Regionen in der Partition automatisch zu aggregieren, sofern Security Hub sie unterstützt und Sie sich für sie entscheiden, wählen Sie future Regionen verknüpfen aus.
8. Wählen Sie Speichern.

Aktivierung der regionsübergreifenden Aggregation (Security Hub API,) AWS CLI

Sie können die Security Hub Hub-API verwenden, um die regionsübergreifende Aggregation zu aktivieren.

Um die regionsübergreifende Aggregation über die Security Hub Hub-API zu aktivieren, erstellen Sie einen Suchaggregator. Sie müssen den Suchaggregator aus der Region erstellen, die Sie als Aggregationsregion verwenden möchten.

Um den Suchaggregator zu erstellen (Security Hub Hub-API, AWS CLI)

- Security Hub Hub-API: Verwenden Sie den `CreateFindingAggregator`Vorgang aus der Region, die Sie als Aggregationsregion verwenden möchten. Für `RegionLinkingMode` wählen Sie aus den folgenden Optionen:
  - `ALL_REGIONS`— Security Hub aggregiert Daten aus allen Regionen. Security Hub aggregiert auch Daten aus neuen Regionen, sofern diese unterstützt werden und Sie sich für diese entscheiden.
  - `ALL_REGIONS_EXCEPT_SPECIFIED`— Security Hub aggregiert Daten aus allen Regionen mit Ausnahme der Regionen, die Sie ausschließen möchten. Security Hub aggregiert auch Daten aus neuen Regionen, sofern diese unterstützt werden und Sie sich für diese entscheiden. Wird verwendet`Regions`, um die Liste der Regionen bereitzustellen, die von der Aggregation ausgeschlossen werden sollen.
  - `SPECIFIED_REGIONS`— Security Hub aggregiert Daten aus einer ausgewählten Liste von Regionen. Security Hub aggregiert Daten aus neuen Regionen nicht automatisch. Wird verwendet`Regions`, um die Liste der Regionen bereitzustellen, aus denen aggregiert werden soll.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl `create-finding-aggregator` aus. Trennen Sie jede Region durch ein Leerzeichen.

```
aws securityhub create-finding-aggregator --region <aggregation Region> --region-
linking-mode ALL_REGIONS | ALL_REGIONS_EXCEPT_SPECIFIED | SPECIFIED_REGIONS --
regions <Region list>
```

Im folgenden Beispiel wird die regionsübergreifende Aggregation für ausgewählte Regionen konfiguriert. Die Aggregationsregion ist USA Ost (Nord-Virginia). Die verknüpften Regionen sind USA West (Nordkalifornien) und USA West (Oregon).

```
aws securityhub create-finding-aggregator --region us-east-1 --region-linking-mode
 SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Regionsübergreifende Aggregationseinstellungen anzeigen

Sie können die aktuelle regionsübergreifende Aggregationskonfiguration von jeder Region aus anzeigen. Die Konfiguration umfasst die Aggregationsregion, die verknüpften Regionen und die Angabe, ob neue Regionen automatisch verknüpft werden sollen.

Anzeige der regionsübergreifenden Aggregationskonfiguration (Konsole)

Auf der Registerkarte „Regionen“ der Seite „Einstellungen“ wird die aktuelle regionsübergreifende Aggregationskonfiguration angezeigt. Sie können die Konfiguration von jeder Region aus anzeigen. Mitgliedskonten können auch die regionsübergreifende Konfiguration anzeigen, die das Administratorkonto konfiguriert hat.

Wenn die regionsübergreifende Aggregation nicht aktiviert ist, wird auf der Registerkarte Regionen die Option zur Aktivierung der regionsübergreifenden Aggregation angezeigt. Siehe the section called “Aktivierung der regionsübergreifenden Aggregation”. Nur Administratorkonten und eigenständige Konten können die regionsübergreifende Aggregation aktivieren.

Wenn die regionsübergreifende Aggregation aktiviert ist, werden auf der Registerkarte Regionen die folgenden Informationen angezeigt:

- Die Aggregationsregion
- Ob Ergebnisse, Erkenntnisse, Kontrollstatus und Sicherheitswerte aus neuen Regionen, die Security Hub unterstützt und für die Sie sich entscheiden, automatisch aggregiert werden sollen
- Die Liste der verknüpften Regionen

Aktuelle regionsübergreifende Aggregationskonfiguration anzeigen (Security Hub Hub-API,) AWS CLI

Sie können die Security Hub Hub-API verwenden oder AWS CLI die aktuelle regionsübergreifende Aggregationskonfiguration anzeigen. Sie können die regionsübergreifende Aggregationskonfiguration von jeder Region aus anzeigen.

Um die aktuelle regionsübergreifende Aggregationskonfiguration anzuzeigen (Security Hub Hub-API,) AWS CLI

- Security Hub Hub-API: Verwenden Sie die `GetFindingAggregator`API. Wenn Sie die Anfrage stellen, müssen Sie den Suchaggregator-ARN angeben. Um den Suchaggregator-ARN zu erhalten, verwenden Sie `ListFindingAggregators`.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl `get-finding-aggregator` aus. Um den Suchaggregator-ARN zu erhalten, verwenden Sie `list-finding-aggregators`.

```
aws securityhub get-finding-aggregator --finding-aggregator-arn <finding aggregator
 ARN>
```

Aktualisierung der regionsübergreifenden Aggregationskonfiguration

Sie können die regionsübergreifende Aggregationskonfiguration aktualisieren, um die verknüpfte Region AWS-Regionen für die aktuelle Aggregation zu ändern. Sie können auch ändern, ob Ergebnisse, Erkenntnisse, Kontrollstatus und Sicherheitsbewertungen aus neuen Regionen automatisch aggregiert werden sollen.

Änderungen an der regionsübergreifenden Aggregation werden für eine Opt-in-Region erst implementiert, wenn die Region in einer aktiviert ist. AWS-Konto Regionen, die am oder nach dem 20. März 2019 AWS eingeführt wurden, sind Opt-in-Regionen.

Wenn Sie die Aggregation von Daten aus einer verknüpften Region beenden, entfernt Security Hub keine vorhandenen aggregierten Daten aus der Aggregationsregion.

Sie können den Aktualisierungsprozess nicht verwenden, um die Aggregationsregion zu ändern. Um die Aggregationsregion zu ändern, müssen Sie wie folgt vorgehen:

1. Beenden Sie die regionsübergreifende Aggregation. Siehe the section called “Die regionsübergreifende Aggregation wird beendet”.
2. Wechseln Sie zu der Region, die Sie als neue Aggregationsregion verwenden möchten.
3. Aktivieren Sie die regionsübergreifende Aggregation. Siehe the section called “Aktivierung der regionsübergreifenden Aggregation”.

Aktualisierung der regionsübergreifenden Aggregationskonfiguration (Konsole)

Sie müssen die regionsübergreifende Aggregationskonfiguration aus der aktuellen Aggregationsregion aktualisieren.

In einer AWS-Regionen anderen Region als der Aggregationsregion wird im Bereich Finding Aggregation eine Meldung angezeigt, dass Sie die Konfiguration in der Aggregationsregion bearbeiten müssen. Wählen Sie diese Meldung, um einen Link anzuzeigen, über den Sie zur Aggregationsregion navigieren können.

Um die verknüpften Regionen für die aktuelle Aggregationsregion zu ändern

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wechseln Sie zur aktuellen Aggregationsregion.
3. Wählen Sie im Security Hub-Navigationsmenü Einstellungen und dann Regionen aus.
4. Wählen Sie unter Aggregation suchen die Option Bearbeiten aus.
5. Aktualisieren Sie unter Verknüpfte Regionen die ausgewählten verknüpften Regionen.
6. Ändern Sie bei Bedarf, ob die Option future Regionen verknüpfen ausgewählt ist. Diese Einstellung bestimmt, ob Security Hub neue Regionen automatisch verknüpft, wenn sie unterstützt werden und Sie sich für sie entscheiden.
7. Wählen Sie Speichern.

Aktualisierung der regionsübergreifenden Aggregationskonfiguration (Security Hub Hub-API,) AWS CLI

Sie können die Security Hub Hub-API verwenden oder AWS CLI die regionsübergreifende Aggregationskonfiguration aktualisieren. Sie müssen die regionsübergreifende Aggregation von der aktuellen Aggregationsregion aus aktualisieren.

Sie können den Modus für die Verknüpfung von Regionen ändern. Wenn der Verbindungsmodus `ALL_REGIONS_EXCEPT_SPECIFIED` oder ist`SPECIFIED_REGIONS`, können Sie die Liste der ausgeschlossenen oder eingeschlossenen Regionen ändern.

Wenn Sie die Liste der ausgeschlossenen oder eingeschlossenen Regionen ändern, müssen Sie die vollständige Liste zusammen mit den Aktualisierungen bereitstellen. Angenommen, Sie aggregieren

derzeit Ergebnisse aus USA Ost (Ohio) und möchten auch Ergebnisse aus USA West (Oregon) aggregieren. Wenn Sie anrufen `UpdateFindingAggregator`, stellen Sie eine `Regions` Liste bereit, die sowohl USA Ost (Ohio) als auch USA West (Oregon) enthält.

Um die regionsübergreifende Aggregation zu aktualisieren (Security Hub API,) AWS CLI

- Security Hub Hub-API: Verwenden Sie den `UpdateFindingAggregator`API-Vorgang. Um den Suchaggregator zu identifizieren, müssen Sie den Suchaggregator-ARN angeben. Um den Suchaggregator-ARN zu erhalten, verwenden Sie `ListFindingAggregators`.

  Sie geben den Regionsverknüpfungsmodus und die aktualisierte Liste der ausgeschlossenen oder eingeschlossenen Regionen an.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl `update-finding-aggregator` aus. Trennen Sie jede Region durch ein Leerzeichen.

  ```
  aws securityhub update-finding-aggregator --region <aggregation Region> --finding-
  aggregator-arn <finding aggregator ARN> --region-linking-mode ALL_REGIONS |
   ALL_REGIONS_EXCEPT_SPECIFIED | SPECIFIED_REGIONS --regions <Region list>
  ```

  Im folgenden Beispiel wird die regionsübergreifende Aggregationskonfiguration auf Aggregation für ausgewählte Regionen geändert. Der Befehl wird von der aktuellen Aggregationsregion aus ausgeführt, nämlich USA Ost (Nord-Virginia). Die verknüpften Regionen sind USA West (Nordkalifornien) und USA West (Oregon).

  ```
  aws securityhub update-finding-aggregator --region us-east-1 --finding-aggregator-arn
   arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-
  a456-426652340000 --region-linking-mode SPECIFIED_REGIONS --regions us-west-1 us-
  west-2
  ```

Die regionsübergreifende Aggregation wird beendet

Beenden Sie die regionsübergreifende Aggregation, wenn Sie keine Daten mehr aggregieren möchten oder wenn Sie die Aggregationsregion ändern möchten.

Wenn Sie die regionsübergreifende Aggregation beenden, beendet Security Hub die Aggregation von Daten. Es entfernt keine vorhandenen aggregierten Daten aus der Aggregationsregion.

Die regionsübergreifende Aggregation wird beendet (Konsole)

Sie müssen die regionsübergreifende Aggregation von der aktuellen Aggregationsregion aus beenden.

In anderen Regionen als der Aggregationsregion wird im Bereich Finding Aggregation eine Meldung angezeigt, dass Sie die Konfiguration in der Aggregationsregion bearbeiten müssen. Wählen Sie diese Meldung, um einen Link anzuzeigen, über den Sie zur Aggregationsregion wechseln können.

Um die regionsübergreifende Aggregation zu beenden

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wechseln Sie zur aktuellen Aggregationsregion.
3. Wählen Sie im Security Hub-Navigationsmenü Einstellungen und dann Regionen aus.
4. Wählen Sie unter Aggregation suchen die Option Bearbeiten aus.
5. Wählen Sie unter Aggregationsregion die Option Keine Aggregationsregion aus.
6. Wählen Sie Speichern.
7. Geben Sie im Bestätigungsdialogfeld in das Bestätigungsfeld Folgendes ein. **`Confirm`**
8. Wählen Sie Bestätigen aus.

Beenden der regionsübergreifenden Aggregation (Security Hub Hub-API,) AWS CLI

Sie können die Security Hub Hub-API verwenden, um die regionsübergreifende Aggregation zu stoppen. Sie müssen die regionsübergreifende Aggregation von der Aggregationsregion aus beenden.

Um die regionsübergreifende Aggregation zu beenden (Security Hub Hub-API,) AWS CLI

- Security Hub Hub-API: Verwenden Sie den `DeleteFindingAggregator`Vorgang. Um den Suchaggregator zu identifizieren, der gelöscht werden soll, geben Sie den Suchaggregator-ARN an. Um den Suchaggregator-ARN zu erhalten, verwenden Sie `ListFindingAggregators`.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl `delete-finding-aggregator` aus.

```
aws securityhub delete-finding-aggregator <finding aggregator ARN> --
region <aggregation Region>
```

Ergebnisse im AWS Security Hub

AWS Security Hub macht die Bearbeitung großer Mengen von Erkenntnissen mehrerer Anbieter überflüssig. Es reduziert den Aufwand, der für die Verwaltung und Verbesserung der Sicherheit all Ihrer AWS-Konten Ressourcen und Workloads erforderlich ist.

Security Hub erhält Ergebnisse aus den folgenden Quellen.

- Security Hub überprüft die aktivierten Kontrollen. Siehe the section called “Generierung und Aktualisierung der Kontrollergebnisse”.
- Integrationen AWS-Services , die Sie aktivieren. Siehe the section called “AWS-Service Integrationen”.
- Integrationen mit Drittanbieterprodukten, die Sie aktivieren. Siehe the section called “Produktintegrationen von Drittanbietern”.
- Benutzerdefinierte Integrationen, die Sie konfigurieren. Siehe the section called “Verwenden benutzerdefinierter Produktintegrationen”.

Security Hub verarbeitet Ergebnisse mithilfe eines Standardergebnisformats, dem sogenannten AWS Security Finding Format. Weitere Informationen über das Ergebnisformat finde Sie unter the section called “Ergebnisformat”.

Security Hub korreliert die Ergebnisse der integrierten Produkte, um die wichtigsten zu priorisieren.

Ergebnisanbieter können Ergebnisse aktualisieren, um zusätzliche Instanzen des Ergebnisses wiederzugeben. Sie können die Ergebnisse aktualisieren, um Details zu Ihrer Untersuchung und ihren Ergebnissen bereitzustellen.

Security Hub ermöglicht es Ihnen auch, Ergebnisse regionsübergreifend zu aggregieren, sodass Sie alle Ihre Ergebnisse von einem Ort aus einsehen können. Siehe Regionsübergreifende Aggregation.

Themen

Ergebnisse erstellen und aktualisieren in AWS Security Hub

AWS Security Hub In kann ein Ergebnis von einem der folgenden Arten von Findungsanbietern stammen.

- Eine aktivierte Sicherheitskontrolle in Security Hub
- Eine aktivierte Integration mit einem anderen AWS-Service
- Eine aktivierte Integration mit einem Drittanbieterprodukt

Nachdem ein Ergebnis erstellt wurde, kann es vom Ergebnisanbieter oder vom Kunden aktualisiert werden.

- Der Ergebnisanbieter verwendet die `BatchImportFindings`-API-Operation, um die allgemeinen Informationen zu einem Ergebnis zu aktualisieren. Ergebnisanbieter können nur Ergebnisse aktualisieren, die sie erstellt haben.
- Der Kunde verwendet den `BatchUpdateFindings`API-Vorgang, um den Status der Untersuchung zu einem Ergebnis zu aktualisieren. `BatchUpdateFindings`kann im Namen des Kunden auch von einem Ticket-, Vorfallmanagement-, Orchestrierungs-, Problembehebungs- oder SIEM-Tool verwendet werden.

  Über die Security Hub Hub-Konsole können Kunden den Workflow-Status von Ergebnissen verwalten und Ergebnisse an benutzerdefinierte Aktionen senden. Siehe the section called “Ergreifen von Maßnahmen aufgrund der Ergebnisse”.

Security Hub aktualisiert und löscht Ergebnisse außerdem automatisch. Alle Ergebnisse werden automatisch gelöscht, wenn sie in den letzten 90 Tagen nicht aktualisiert wurden.

Wenn Sie die regionsübergreifende Aggregation aktivieren, aggregiert Security Hub automatisch neue Ergebnisse aus den verknüpften Regionen in die Aggregationsregion. Security Hub repliziert auch Aktualisierungen der Ergebnisse. Updates, die in den verknüpften Regionen auftreten, werden in die Aggregationsregion repliziert. Aktualisierungen, die in der Aggregationsregion vorgenommen werden, werden in die verknüpfte Region repliziert. Weitere Informationen zur regionsübergreifenden Aggregation finden Sie unter. Regionsübergreifende Aggregation

Themen

Verwenden von BatchImportFindings zum Erstellen und Aktualisieren von Ergebnissen

Ergebnisanbieter verwenden die `BatchImportFindings`-API-Operation, um neue Ergebnisse zu erstellen und Informationen über die von ihnen erstellten Ergebnisse zu aktualisieren. Sie können keine Ergebnisse aktualisieren, die sie nicht erstellt haben.

Kunden, SIEMs, Ticketing-Tools und SOAR-Tools verwenden, `BatchUpdateFindings`um Aktualisierungen im Zusammenhang mit ihrer Untersuchung der Ergebnisse von Finding Providern vorzunehmen. Siehe the section called “Verwenden von BatchUpdateFindings”.

Immer AWS Security Hub wenn eine `BatchImportFindings` Anfrage zur Erstellung oder Aktualisierung eines Ergebnisses eingeht, wird automatisch ein Security Hub Findings - ImportedEreignis in Amazon generiert EventBridge. Siehe the section called “Automatisierte Reaktion und Problembehebung”.

Anforderungen an Konten und Chargengröße

`BatchImportFindings`muss von einem der folgenden Anbieter aufgerufen werden:

- Das Konto, das mit den Ergebnissen verknüpft ist. Die Kennung des zugehörigen Kontos ist der Wert des `AwsAccountId` Attributs für den Befund.
- Ein Konto, das auf der Zulassungsliste für eine offizielle Security Hub-Partnerintegration steht.

Security Hub kann nur die Suche nach Updates für Konten akzeptieren, für die Security Hub aktiviert ist. Der Ergebnisanbieter muss ebenfalls aktiviert sein. Wenn Security Hub deaktiviert oder die Finding Provider-Integration nicht aktiviert ist, werden die Ergebnisse in der `FailedFindings` Liste mit einem `InvalidAccess` Fehler zurückgegeben.

`BatchImportFindings`akzeptiert bis zu 100 Ergebnisse pro Stapel, bis zu 240 KB pro Ergebnis und bis zu 6 MB pro Stapel. Die Drosselungsrate ist auf 10 TPS pro Konto und Region begrenzt, bei einem Burst-Wert von 30 TPS.

Festlegen, ob ein Ergebnis erstellt oder aktualisiert werden soll

Um festzustellen, ob ein Ergebnis erstellt oder aktualisiert werden soll, überprüft Security Hub das `ID` Feld. Wenn der Wert von `ID` nicht mit einem vorhandenen Ergebnis übereinstimmt, wird ein neues Ergebnis erstellt.

Wenn `ID` dies mit einem vorhandenen Ergebnis übereinstimmt, überprüft Security Hub das `UpdatedAt` Feld auf das Update.

- Wenn `UpdatedAt` das Update mit `UpdatedAt` dem vorhandenen Ergebnis übereinstimmt oder vorher auftritt, wird das Update ignoriert.
- Wenn `UpdatedAt` bei der Aktualisierung nach `UpdatedAt` des vorhandenen Ergebnisses auftritt, wird das vorhandene Ergebnis aktualisiert.

Eingeschränkte Attribute für BatchImportFindings

Bei einem vorhandenen Befund können Suchprovider die folgenden Attribute und Objekte nicht aktualisieren. `BatchImportFindings` Diese Attribute können nur mit aktualisiert werden`BatchUpdateFindings`.

- `Note`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Security Hub ignoriert alle Inhalte, die in einer `BatchImportFindings` Anfrage für diese Attribute und Objekte bereitgestellt werden. Kunden oder andere Anbieter, die in ihrem Namen handeln, verwenden, um sie `BatchUpdateFindings` zu aktualisieren.

Verwenden von FindingProviderFields

Die Suche nach Anbietern sollte auch nicht verwendet `BatchImportFindings` werden, um die folgenden Attribute zu aktualisieren.

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

Stattdessen verwendet die Suche nach Anbietern das `FindingProviderFields`Objekt, um Werte für diese Attribute bereitzustellen.

Beispiel

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

Bei `BatchImportFindings` Anfragen verarbeitet Security Hub Werte in den Attributen der obersten Ebene und `FindingProviderFields`wie folgt.

(Preferred) **`BatchImportFindings`** stellt einen Wert für ein Attribut in **`FindingProviderFields`**, aber keinen Wert für das entsprechende Attribut der obersten Ebene bereit.

Zum Beispiel `BatchImportFindings` liefert`FindingProviderFields.Confidence`, aber nicht. `Confidence` Dies ist die bevorzugte Option für `BatchImportFindings` Anfragen.

Security Hub aktualisiert den Wert des Attributs in`FindingProviderFields`.

Es repliziert den Wert nur dann in das Attribut der obersten Ebene, wenn das Attribut nicht bereits von aktualisiert wurde. `BatchUpdateFindings`

`BatchImportFindings`liefert einen Wert für ein Attribut der obersten Ebene, aber keinen Wert für das entsprechende Attribut in. **`FindingProviderFields`**

Stellt beispielsweise `BatchImportFindings` bereit`Confidence`, liefert aber nicht. `FindingProviderFields.Confidence`

Security Hub verwendet den Wert, um das Attribut in zu aktualisieren`FindingProviderFields`. Es überschreibt jeden vorhandenen Wert.

Security Hub aktualisiert das Attribut der obersten Ebene nur, wenn das Attribut nicht bereits von `BatchUpdateFindings` aktualisiert wurde.

`BatchImportFindings`stellt einen Wert sowohl für ein Attribut der obersten Ebene als auch für das entsprechende Attribut in bereit. **`FindingProviderFields`**

`BatchImportFindings`Stellt beispielsweise sowohl als auch `Confidence` bereit. `FindingProviderFields.Confidence`

Bei einem neuen Befund verwendet Security Hub den Wert in, `FindingProviderFields` um sowohl das Attribut der obersten Ebene als auch das entsprechende Attribut in aufzufüllen. `FindingProviderFields` Der angegebene Attributwert der obersten Ebene wird nicht verwendet.

Für ein vorhandenes Ergebnis verwendet Security Hub beide Werte. Der Attributwert der obersten Ebene wird jedoch nur aktualisiert, wenn das Attribut nicht bereits von `BatchUpdateFindings` aktualisiert wurde.

Verwenden Sie den batch-import-findings Befehl aus dem AWS CLI

In der verwenden Sie den `batch-import-findings`Befehl AWS Command Line Interface, um Ergebnisse zu erstellen oder zu aktualisieren.

Sie stellen jedes Ergebnis als JSON-Objekt bereit.

Beispiel

```
aws securityhub batch-import-findings --findings
    [{
        "AwsAccountId": "123456789012",
        "CreatedAt": "2019-08-07T17:05:54.832Z",
        "Description": "Vulnerability in a CloudTrail trail",
        "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0/rule/2.2",
        "Id": "Id1",
        "ProductArn": "arn:aws:securityhub:us-west-1:123456789012:product/123456789012/
default",
        "Resources": [
            {
                "Id": "arn:aws:cloudtrail:us-west-1:123456789012:trail/TrailName",
                "Partition": "aws",
                "Region": "us-west-1",
                "Type": "AwsCloudTrailTrail"
            }
```

```
        ],
        "SchemaVersion": "2018-10-08",
        "Title": "CloudTrail trail vulnerability",
        "UpdatedAt": "2020-06-02T16:05:54.832Z",
        "Types": [
            "Software and Configuration Checks/Vulnerabilities/CVE"
        ],
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "0"
        }
    }]'
```

Verwenden von BatchUpdateFindings, um ein Ergebnis zu aktualisieren

Die `BatchUpdateFindings`Aktion wird verwendet, um Informationen zu aktualisieren, die sich auf die Verarbeitung von Ergebnissen aus der Suche nach Anbietern durch einen Kunden beziehen. Sie kann von einem Kunden oder von einem SIEM-, Ticketing-, Incident Management- oder SOAR-Tool verwendet werden, das im Auftrag eines Kunden arbeitet. Sie können `BatchUpdateFindings` es verwenden, um bestimmte Felder im AWS Security Finding Format (ASFF) zu aktualisieren.

Sie können es nicht verwenden`BatchUpdateFindings`, um neue Ergebnisse zu erstellen. Sie können damit bis zu 100 Ergebnisse gleichzeitig aktualisieren.

Immer wenn Security Hub eine `BatchUpdateFindings` Anfrage zur Aktualisierung eines Ergebnisses erhält, generiert es automatisch ein Security Hub Findings - ImportedEreignis in Amazon EventBridge. Siehe the section called “Automatisierte Reaktion und Problembehebung”.

`BatchUpdateFindings`ändert das `UpdatedAt` Feld für den Befund nicht. `UpdatedAt`spiegelt nur das neueste Update des Findungsanbieters wider.

Verfügbare Felder für BatchUpdateFindings

Administratorkonten können > verwenden`BatchUpdateFindings`, um die Ergebnisse für ihr Konto oder ihre Mitgliedskonten zu aktualisieren. Mitgliedskonten können > verwenden`BatchUpdateFindings`, um die Ergebnisse für ihr Konto zu aktualisieren.

Kunden können > nur verwenden`BatchUpdateFindings`, um die folgenden Felder und Objekte zu aktualisieren.

- `Confidence`

- `Criticality`
- `Note`
- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Standardmäßig haben Administrator- und Mitgliedskonten Zugriff auf alle oben genannten Felder und Feldwerte. Security Hub bietet auch Kontextschlüssel, mit denen Sie den Zugriff auf Felder und Feldwerte einschränken können.

Beispielsweise können Sie nur Mitgliedskonten die Einstellung auf `Workflow.Status` erlaubenRESOLVED. Oder Sie möchten möglicherweise nicht zulassen, dass sich Mitgliedskonten ändern`Severity.Label`.

Konfiguration des Zugriffs auf BatchUpdateFindings

Sie können IAM-Richtlinien konfigurieren, um den Zugriff auf die Verwendung `BatchUpdateFindings` zur Aktualisierung von Feldern und Feldwerten zu beschränken.

Verwenden Sie in einer Anweisung, auf die der Zugriff beschränkt werden soll`BatchUpdateFindings`, die folgenden Werte:

- `Action` ist `securityhub:BatchUpdateFindings`
- `Effect` ist `Deny`
- Denn `Condition` Sie können eine `BatchUpdateFindings` Anfrage auf folgender Grundlage ablehnen:
  - Das Ergebnis umfasst ein bestimmtes Feld.
  - Das Ergebnis beinhaltet einen bestimmten Feldwert.

Bedingungsschlüssel

Dies sind die Bedingungsschlüssel für die Einschränkung des Zugriffs auf`BatchUpdateFindings`.

ASFF-Feld

Der Bedingungsschlüssel für ein ASFF-Feld lautet wie folgt:

```
securityhub:ASFFSyntaxPath/<fieldName>
```

Ersetzen Sie es *<fieldName>* durch das ASFF-Feld. Fügen Sie bei der Konfiguration des Zugriffs auf `BatchUpdateFindings` ein oder mehrere spezifische ASFF-Felder in Ihre IAM-Richtlinie ein und nicht ein Feld auf übergeordneter Ebene. Um beispielsweise den Zugriff auf das `Workflow.Status` Feld einzuschränken, müssen Sie es `securityhub:ASFFSyntaxPath/Workflow.Status` in Ihre Richtlinie aufnehmen und nicht das Feld auf übergeordneter Ebene. `Workflow`

Alle Aktualisierungen eines Felds verbieten

Um zu verhindern, dass ein Benutzer ein bestimmtes Feld aktualisiert, verwenden Sie eine Bedingung wie die folgende:

```
 "Condition": {
                "Null": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "false"
               }
}
```

Die folgende Anweisung weist beispielsweise darauf hin, dass der Workflow-Status nicht aktualisiert werden `BatchUpdateFindings` kann.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
        "Null": {
            "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
        }
    }
}
```

Bestimmte Feldwerte nicht zulassen

Um zu verhindern, dass ein Benutzer ein Feld auf einen bestimmten Wert setzt, verwenden Sie eine Bedingung wie die folgende:

```
"Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
                }
}
```

Die folgende Anweisung weist beispielsweise darauf hin, dass diese Einstellung nicht verwendet werden `BatchUpdateFindings` kann, um auf `Workflow.Status` zu setzen`SUPPRESSED`.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
}
```

Sie können auch eine Liste mit Werten angeben, die nicht zulässig sind.

```
 "Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
 "<fieldValue2>", "<fieldValuen>" ]
                }
}
```

Die folgende Anweisung weist beispielsweise darauf hin, dass dieser Wert nicht verwendet werden `BatchUpdateFindings` kann, um entweder `Workflow.Status` auf `RESOLVED` oder zu setzen`SUPPRESSED`.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
```

```
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": [
            "RESOLVED",
            "NOTIFIED"
        ]
    }
}
```

Verwenden Sie den batch-update-findings Befehl von AWS CLI

In der verwenden Sie den `batch-update-findings`Befehl AWS Command Line Interface, um die Ergebnisse zu aktualisieren.

Für jedes Ergebnis, das aktualisiert werden soll, geben Sie sowohl die Ergebnis-ID als auch den ARN des Produkts an, das den Befund generiert hat.

```
--finding-identifiers ID="<findingID1>",ProductArn="<productARN>"
 ID="<findingID2>",ProductArn="<productARN2>"
```

Wenn Sie die zu aktualisierenden Attribute angeben, können Sie entweder ein JSON-Format oder ein Shortcut-Format verwenden.

Hier ist ein Beispiel für eine Aktualisierung des `Note` Objekts, das das JSON-Format verwendet:

```
--note '{"Text": "Known issue that is not a risk.", "UpdatedBy": "user1"}'
```

Hier ist dasselbe Update, das das Shortcut-Format verwendet:

```
--note Text="Known issue that is not a risk.",UpdatedBy="user1"
```

Die AWS CLI Befehlsreferenz enthält die JSON- und Shortcut-Syntax für jedes Feld.

Im folgenden `batch-update-findings` Beispiel > werden zwei Ergebnisse aktualisiert, um eine Notiz hinzuzufügen, die Bezeichnung für den Schweregrad zu ändern und die Fehler zu beheben.

```
aws securityhub batch-update-findings --finding-identifiers Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
```

```
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2::product/aws/securityhub" Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" --note '{"Text": "Known issue that is not a
 risk.", "UpdatedBy": "user1"}' --severity '{"Label": "LOW"}' --workflow '{"Status":
 "RESOLVED"}'
```

Dies ist dasselbe Beispiel, verwendet jedoch die Abkürzungen anstelle von JSON.

```
aws securityhub batch-update-findings --finding-identifiers Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" --note Text="Known issue that is not a
 risk.",UpdatedBy="user1" --severity Label="LOW" --workflow Status="RESOLVED"
```

Verwaltung und Überprüfung der Funddetails und des Verlaufs

Es gibt mehrere Möglichkeiten, Suchlisten auf der AWS Security Hub Konsole anzuzeigen:

- Ergebnisseite — Zeigt eine umfassende Liste der Ergebnisse aller aktivierten Steuerungen und Produktintegrationen an. Standardmäßig werden aktive Ergebnisse mit dem `NOTIFIED` Workflow-Status `NEW` oder angezeigt.
- Seite mit Kontrolldetails — Zeigt eine Liste der Ergebnisse an, die in den letzten 24 Stunden für eine bestimmte Kontrolle generiert wurden.
- Seite „Einblicke“ — Zeigt eine Liste mit Ergebnissen für einen passenden Einblick an. Bei einem Einblick handelt es sich um sammlungsspezifische Ergebnisse. Weitere Informationen finden Sie unter the section called “Anzeigen von Insight-Ergebnissen und -Resultaten”.
- Seite „Integrationen“ — Zeigt eine Liste der Ergebnisse an, die von einem integrierten Produkt AWS-Service oder einem Drittanbieterprodukt generiert wurden.

Sie können die Ergebnisse in diesen Listen filtern und gruppieren, um sich auf bestimmte Arten von Ergebnissen zu konzentrieren. Sie können auch ein bestimmtes Ergebnis auf den vorherigen Seiten auswählen, um Details zu diesem Ergebnis anzuzeigen.

Um eine Liste der Ergebnisse programmgesteuert anzuzeigen, verwenden Sie den `GetFindings`Betrieb der Security Hub Hub-API. Sie können Filter einbeziehen, um bestimmte Arten von Ergebnissen abzurufen.

Wenn Sie die regionsübergreifende Aggregation aktivieren, können Sie Kontrollstatus, Sicherheitswerte, Erkenntnisse und Ergebnisse aus verschiedenen Regionen abrufen. In der Aggregationsregion umfasst das Auffinden von Daten Daten aus der Aggregationsregion und den verknüpften Regionen. In anderen Regionen ist das Auffinden von Daten nur für diese Region spezifisch. Hinweise zur Konfiguration der regionsübergreifenden Aggregation finden Sie unter. Regionsübergreifende Aggregation

Ergebnisse filtern und gruppieren (Konsole)

Wenn Sie eine Ergebnisliste auf der Seite Ergebnisse, Integrationen oder Einblicke der Security Hub Hub-Konsole anzeigen, wird die Liste anhand des Datensatzstatus und des Workflow-Status vorgefiltert. Dies gilt zusätzlich zu den Filtern für einen Einblick oder eine Integration.

Der Datensatzstatus gibt an, ob ein Ergebnis aktiv oder archiviert ist. Standardmäßig werden in einer Ergebnisliste nur aktive Ergebnisse angezeigt. Ein Befund kann vom Befundanbieter archiviert werden. AWS Security Hub archiviert auch automatisch Kontrollergebnisse, wenn die zugehörige Ressource gelöscht wird.

Der Workflow-Status gibt den Status einer Untersuchung eines Ergebnisses an. Standardmäßig werden in einer Ergebnisliste nur Ergebnisse mit dem Workflow-Status `NEW` oder `NOTIFIED` angezeigt. Sie können den Workflow-Status eines Ergebnisses aktualisieren.

Wenn Sie die Aggregation von Ergebnissen aktiviert haben und in der Aggregationsregion angemeldet sind, können Sie die Ergebnisse auf den Seiten Ergebnisse und Einblicke nach Regionen filtern.

Informationen zum Arbeiten mit Kontrollergebnissen finden Sie unter. the section called “Ergebnisse filtern und sortieren” Die Informationen auf dieser Seite beziehen sich auf die Ergebnislisten auf den Seiten Ergebnisse, Einblicke und Integrationen.

Hinzufügen von Filtern

Um den Bereich der Liste zu ändern, können Sie Filter hinzufügen.

Sie können nach bis zu 10 Attributen filtern. Für jedes Attribut können Sie bis zu 20 Filterwerte angeben.

Beim Filtern der Ergebnisliste wendet Security Hub die UND-Logik auf den Filtersatz an. Mit anderen Worten: Eine Suche stimmt nur dann überein, wenn sie mit allen bereitgestellten Filtern übereinstimmt. Wenn Sie beispielsweise einen Filter für den Produktnamen und `AwsS3Bucket` als Filter für den Ressourcentyp hinzufügen GuardDuty , müssen die übereinstimmenden Ergebnisse diesen beiden Kriterien entsprechen.

Security Hub wendet jedoch die OR-Logik auf Filter an, die dasselbe Attribut, aber unterschiedliche Werte verwenden. Sie fügen beispielsweise GuardDuty sowohl als auch Amazon Inspector als Filterwerte für den Produktnamen hinzu. In diesem Fall stimmt ein Ergebnis überein, wenn es entweder von Amazon Inspector GuardDuty oder von Amazon Inspector generiert wurde.

So fügen Sie der Ergebnisliste einen Filter hinzu

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Gehen Sie wie folgt vor, um eine Ergebnisliste anzuzeigen:
   - Wählen Sie im Security Hub-Navigationsbereich Findings aus.
   - Wählen Sie im Security Hub-Navigationsbereich Insights aus. Wählen Sie einen Einblick aus. Wählen Sie dann in der Ergebnisliste ein Insight-Ergebnis aus.
   - Wählen Sie im Security Hub-Navigationsbereich Integrationen aus. Wählen Sie Ergebnisse für eine Integration anzeigen aus.
3. Wählen Sie im Feld Filter hinzufügen für Filter einen Filter aus.

   Wenn Sie nach Firmenname oder Produktname filtern, verwendet die Konsole die `ProductName` Felder `CompanyName` und auf oberster Ebene. Die API verwendet die Werte, die sich in `ProductFields` befinden.
4. Wählen Sie den Filterübereinstimmungstyp aus.

   Für einen Zeichenkettenfilter können Sie aus den folgenden Vergleichsoptionen wählen:

   - ist — Findet einen Wert, der genau dem Filterwert entspricht.
   - beginnt mit — Findet einen Wert, der mit dem Filterwert beginnt.
   - ist nicht — Findet einen Wert, der nicht mit dem Filterwert übereinstimmt.
   - beginnt nicht mit — Findet einen Wert, der nicht mit dem Filterwert beginnt.

   Bei einem numerischen Filter können Sie wählen, ob Sie eine einzelne Zahl (Einfach) oder einen Zahlenbereich (Bereich) angeben möchten.

Für einen Datums- oder Uhrzeitfilter können Sie wählen, ob Sie eine Zeitspanne vom aktuellen Datum und der aktuellen Uhrzeit (Rollendes Fenster) oder einen bestimmten Datumsbereich (fester Bereich) angeben möchten.

Das Hinzufügen mehrerer Filter hat die folgenden Interaktionen:

- ist und beginnt mit Filtern werden durch OR verknüpft. Ein Wert stimmt überein, wenn er einen der Filterwerte enthält. Wenn Sie beispielsweise die Bezeichnung Schweregrad auf KRITISCH und die Bezeichnung Schweregrad auf HOCH angeben, enthalten die Ergebnisse sowohl kritische als auch Ergebnisse mit hohem Schweregrad.
- ist nicht und beginnt auch nicht mit Filtern, die durch UND verknüpft werden. Ein Wert stimmt nur überein, wenn er keinen dieser Filterwerte enthält. Wenn Sie beispielsweise angeben, dass die Bezeichnung Schweregrad nicht NIEDRIG und die Bezeichnung Schweregrad nicht MITTEL ist, enthalten die Ergebnisse keine Ergebnisse mit niedrigem oder mittlerem Schweregrad.

Wenn Sie einen Is-Filter für ein Feld verwenden, können Sie nicht den Filter Ist nicht oder A fängt nicht mit an für dasselbe Feld verwenden.

5. Geben Sie den Filterwert an.

   Bei Zeichenkettenfiltern unterscheidet der Filterwert zwischen Groß- und Kleinschreibung.

   Für Ergebnisse aus Security Hub lautet der Produktname beispielsweise Security Hub. Wenn Sie den EQUALS-Operator verwenden, um Ergebnisse von Security Hub anzuzeigen, müssen Sie **`Security Hub`** als Filterwert eingeben. Wenn Sie **`security hub`** eingeben, werden keine Ergebnisse angezeigt.

   Ebenso werden die Security Hub Hub-Ergebnisse angezeigt, wenn Sie den PREFIX-Operator verwenden und eingeben**`Sec`**. Wenn Sie eingeben**`sec`**, werden keine Security Hub Hub-Ergebnisse angezeigt.

6. Wählen Sie Apply (Anwenden) aus.

Gruppieren der Ergebnisse

Sie können nicht nur die Filter ändern, sondern auch die Ergebnisse anhand der Werte eines ausgewählten Attributs gruppieren.

Wenn Sie die Ergebnisse gruppieren, wird die Ergebnisliste durch eine Werteliste für das ausgewählte Attribut in den entsprechenden Ergebnissen ersetzt. Für jeden Wert zeigt die Liste die Anzahl der Ergebnisse an, die den anderen Filterkriterien entsprechen.

Wenn Sie die Ergebnisse beispielsweise nach AWS-Konto ID gruppieren, wird eine Liste von Konto-IDs mit der Anzahl der übereinstimmenden Ergebnisse für jedes Konto angezeigt.

Beachten Sie, dass Security Hub nur 100 Werte anzeigen kann. Wenn es mehr als 100 Gruppierungswerte gibt, werden nur die ersten 100 angezeigt.

Wenn Sie einen Attributwert auswählen, wird die Liste der passenden Ergebnisse für diesen Wert angezeigt.

So gruppieren Sie die Ergebnisse in einer Ergebnisliste

1. Wählen Sie in der Ergebnisliste das Feld Filter hinzufügen aus.
2. Wählen Sie für Gruppierung die Option Gruppieren nach aus.
3. Wählen Sie in der Liste das Attribut aus, das für die Gruppierung verwendet werden soll.
4. Wählen Sie Apply (Anwenden) aus.

Ändern eines Filterwerts oder eines Gruppierungsattributs

Bei einem vorhandenen Filter können Sie den Filterwert ändern. Sie können das Gruppierungsattribut auch ändern.

Beispielsweise können Sie den Filter Record state (Datensatzstatus) so ändern, dass er nach `ARCHIVED`-Ergebnissen anstelle von `ACTIVE`-Ergebnissen sucht.

Um ein Filter- oder Gruppierungsattribut zu bearbeiten

1. Wählen Sie in einer gefilterten Ergebnisliste das Filter- oder Gruppierungsattribut aus.
2. Wählen Sie für Gruppieren nach das neue Attribut aus und klicken Sie dann auf Anwenden.
3. Wählen Sie für einen Filter den neuen Wert aus und klicken Sie dann auf Anwenden.

Löschen eines Filter- oder Gruppierungsattributs

Um ein Filter- oder Gruppierungsattribut zu löschen, wählen Sie das X-Symbol.

Die Liste wird automatisch aktualisiert, um die Änderung widerzuspiegeln. Wenn Sie das Gruppierungsattribut entfernen, ändert sich die Liste von der Liste der Feldwerte wieder in eine Ergebnisliste.

Verfügbare Suchinformationen

Sie können eine Vielzahl von Ergebnisdetails auf der Security Hub Hub-Konsole oder durch Aufrufen des GetFindingsBetriebs der Security Hub Hub-API abrufen. Hier ist eine unvollständige Liste der Arten von Suchdetails, die Sie abrufen können.

- Anwendungsmetadaten — Geben den Namen und den Amazon-Ressourcennamen (ARN) der Anwendung an, die an einer Suche beteiligt war, falls Sie eine Anwendung erstellt und ihr das AWS Anwendungs-Tag hinzugefügt haben. Wir empfehlen, Anwendungen in AWS Service Catalog AppRegistryzu erstellen.
- Fundverlauf — Zeigt den Verlauf des Fundes in den letzten 90 Tagen an.
- Finding Investigation in Detective (nur Konsole) — Stellt einen Link zur Verfügung, um ein Ergebnis in Detective mithilfe automatisierter Tools zur Protokollerfassung, Sicherheitsanalyse und AWS-Service Ressourcenerkundung weiter zu untersuchen. Diese Informationen sind nur für Security Hub Hub-Ergebnisse enthalten, die von anderen erhalten wurden AWS-Services , wenn Sie Detective aktivieren.
- Felder für die Suche nach Anbietern — Zeigt die Werte des Suchproviders für Zuverlässigkeit, Kritikalität, verwandte Ergebnisse, Schweregrad und Art des Ergebnisses an.
- Parameter — Zeigt die aktuellen Parameterwerte für eine Sicherheitskontrolle an. Security Hub verwendet diese Parameterwerte bei der Durchführung von Sicherheitsprüfungen der Steuerung.
- Behebung — Stellt einen Link zu den Anweisungen zur Behebung fehlgeschlagener Kontrollergebnisse bereit.
- Ressource — Stellt Informationen über die AWS Ressource bereit, die an einem Befund beteiligt war.
- Ressourcen-Tags — Stellt Informationen zu Tag-Schlüsseln und -Werten für die Ressourcen bereit, die an einem Ergebnis beteiligt sind. Sie können Ressourcen taggen, die vom `GetResources` Betrieb der AWS Resource Groups Tagging-API unterstützt werden. Weitere Informationen zur Aufnahme von Ressourcen-Tags in Ergebnisse finden Sie unterTags.
- Typen und zugehörige Ergebnisse — Enthält Informationen zum Befundtyp.
- Details zur Sicherheitslücke — Informationen zu einer Sicherheitslücke, die in einem Befund entdeckt wurde, und zu den betroffenen Paketen. Diese Details sind verfügbar, wenn Sie Amazon Inspector für Ergebnisse aktivieren, die Amazon Inspector an Security Hub sendet.

Lesen Sie die folgenden Abschnitte, um zu erfahren, wie Sie auf diese Details zugreifen können, um ein Ergebnis zu ermitteln.

Den Verlauf der Ergebnisse überprüfen

Der Suchverlauf ist eine Security Hub Hub-Funktion, mit der Sie Änderungen verfolgen können, die in den letzten 90 Tagen an einem Ergebnis vorgenommen wurden. Sie ist für aktive und archivierte Ergebnisse verfügbar. Die Fundhistorie bietet eine unveränderliche Aufzeichnung der Änderungen, die im Laufe der Zeit an einem Ergebnis vorgenommen wurden, einschließlich der Art der Änderung, des Zeitpunkts und des Benutzers.

Insbesondere können Sie Änderungen nachverfolgen, die an Feldern in der AWS Format für Sicherheitssuche (ASFF) vorgenommen wurden. Security Hub verfolgt Änderungen, die Sie manuell und mit Automatisierungsregeln vornehmen.

Der Suchverlauf ist in der Security Hub Hub-Konsole, der API und verfügbar AWS CLI.

Wenn Sie mit einem Security Hub-Administratorkonto angemeldet sind, können Sie den Suchverlauf für das Administratorkonto und alle Mitgliedskonten abrufen.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um den Suchverlauf zu überprüfen.

Security Hub console

Den Suchverlauf überprüfen

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im linken Navigationsbereich Findings aus.
3. Wählen Sie ein Ergebnis aus. Wählen Sie im daraufhin angezeigten Fenster die Registerkarte Verlauf aus.

Security Hub API

Den Suchverlauf überprüfen

1. Führen Sie den Befehl aus GetFindings, oder wenn Sie den verwenden AWS CLI, führen Sie den get-findingsBefehl aus. Verwenden Sie bei Bedarf die entsprechenden Filter, um

das Ergebnis zu identifizieren, für das Sie den Verlauf anzeigen möchten. In der API-Antwort erhalten Sie das `ProductArn` und `Id` für das Ergebnis. Sie benötigen die Werte für diese Felder im dritten Schritt.

2. Führen Sie den Befehl aus GetFindingHistory, oder wenn Sie den verwenden AWS CLI, führen Sie den get-finding-historyBefehl aus.
3. Identifizieren Sie das Ergebnis, für das Sie den Verlauf abrufen möchten, mit den `Id` Feldern `ProductArn` und. Weitere Informationen zu diesen Feldern finden Sie unter AwsSecurityFindingIdentifier. Sie können pro Anfrage nur den Verlauf für einen Befund abrufen.
4. Geben Sie Werte für`StartTime`... `EndTime` an und beschränken Sie den Suchverlauf auf einen bestimmten Zeitraum.
5. Geben Sie einen Wert `MaxResults` an, um den Suchverlauf auf eine bestimmte Anzahl von Ergebnissen zu beschränken. Falls nicht angegeben, gibt die API-Antwort die ersten 100 Ergebnisse des Suchverlaufs zurück.
6. Geben Sie einen Wert für ein`NextToken`, um die nächsten 100 Ergebnisse (falls zutreffend) für einen Befund anzuzeigen. In Ihrer ersten API-Anfrage `NextToken` sollte der Wert von sein`NULL`.

Der folgende CLI-Befehl ruft den Verlauf für den angegebenen Befund ab. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub get-finding-history \
--region us-west-2 \
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2:123456789012:product/123456789012/default" \
--max-results 2 \
--start-time "2021-09-30T15:53:35.573Z" \
--end-time "2021-09-31T15:53:35.573Z"
```

Details zu den Ergebnissen werden überprüft

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um die Suchdetails in Security Hub anzuzeigen.

Security Hub console

Einzelheiten zu den Ergebnissen überprüfen

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Um eine Ergebnisliste anzuzeigen, führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie im Security Hub-Navigationsbereich Findings aus. Fügen Sie nach Bedarf Suchfilter hinzu, um die Ergebnisliste einzugrenzen.
   - Wählen Sie im Security Hub-Navigationsbereich Insights aus. Wählen Sie einen Einblick aus. Wählen Sie dann in der Ergebnisliste ein Insight-Ergebnis aus.
   - Wählen Sie im Security Hub-Navigationsbereich Integrationen aus. Wählen Sie Ergebnisse für eine Integration anzeigen aus.
3. Wählen Sie einen Titel für das Ergebnis aus.
4. Im Bereich mit den Details zu den Ergebnissen können Sie wie folgt weitere Aktionen ausführen:
   - Um die vollständige JSON-Datei für den Befund anzuzeigen, wählen Sie die Ergebnis-ID aus. Laden Sie unter Finding JSON den Finding JSON herunter.
   - Für Ergebnisse, die auf AWS Config Regeln basieren, wählen Sie Regeln aus, um eine Liste der geltenden Regeln anzuzeigen.
   - Wählen Sie Investigate with Macie aus, um sensible Daten zu untersuchen, die im Ergebnis in der Macie-Konsole entdeckt wurden. Diese Option ist nur verfügbar, wenn Sie Amazon Macie und seine automatische Erkennungsfunktion für sensible Daten aktivieren.
   - Wählen Sie Ressourcen, um Informationen über die Ressource anzuzeigen, die an einem Befund beteiligt war.
   - Wählen Sie Investigate in Amazon Detective, um das Ergebnis in der Detective-Konsole zu untersuchen. Diese Option ist nur verfügbar, wenn Sie Amazon Detective aktivieren.
   - Wählen Sie die Registerkarte Verlauf, um den Suchverlauf von bis zu 90 Tagen anzuzeigen.

> **Note**
>
> Oben im Bereich mit den Befunddetails finden Sie Übersichtsinformationen über das Ergebnis, einschließlich Konto, Schweregrad, Datum und Status. Wenn Sie eine

Integration durchführen AWS Organizations und es sich bei dem Konto, bei dem Sie angemeldet sind, um ein Mitgliedskonto der Organisation handelt, enthält der Detailbereich den Kontonamen. Für Mitgliedskonten, die manuell und nicht über die Organisationsintegration eingeladen werden, enthält der Detailbereich nur die Konto-ID.

Security Hub API

Die Details zu den Ergebnissen werden überprüft

Verwenden Sie den `GetFindings`Betrieb der Security Hub Hub-API, oder wenn Sie den verwenden AWS CLI, führen Sie den Befehl get-findings aus.

Sie können einen oder mehrere Werte für den `Filters` Parameter angeben, um die Ergebnisse einzugrenzen, die Sie abrufen möchten.

Wenn das Volumen der Ergebnisse zu groß ist, können Sie den `MaxResults` Parameter verwenden, um die Ergebnisse auf eine bestimmte Anzahl zu beschränken, und den `NextToken` Parameter, um die Ergebnisse zu paginieren. Verwenden Sie den `SortCriteria` Parameter, um die Ergebnisse nach einem bestimmten Feld zu sortieren.

Wenn Sie die regionsübergreifende Aggregation aktiviert haben und diesen Vorgang von der Aggregationsregion aus aufrufen, enthalten die Ergebnisse Ergebnisse aus der Aggregation und verknüpften Regionen.

Der folgende CLI-Befehl ruft die Ergebnisse ab, die den bereitgestellten Filtern entsprechen, und sortiert sie in absteigender Reihenfolge des `LastObservedAt` Felds. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securityhub get-findings \
--filters '{"GeneratorId":[{"Value": "aws-
foundational","Comparison":"PREFIX"}],"WorkflowStatus": [{"Value":
 "NEW","Comparison":"EQUALS"}],"Confidence": [{"Gte": 85}]}' --sort-criteria
 '{"Field": "LastObservedAt","SortOrder": "desc"}' --page-size 5 --max-items 100
```

PowerShell

Die Details zu den Ergebnissen werden überprüft

1. Verwenden Sie das `Get-SHUBFinding` Cmdlet.

2. Füllen Sie optional den `Filter` Parameter aus, um die Ergebnisse einzugrenzen, die Sie abrufen möchten.

Beispiel

```
Get-SHUBFinding -Filter @{AwsAccountId =
 [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =
 "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =
 "EQUALS"; Value = 'FAILED'}}
```

> **Note**
>
> Wenn Sie Ergebnisse nach `CompanyName` oder filtern`ProductName`, verwendet Security Hub die Werte, die Teil des `ProductFields` ASFF-Objekts sind. Security Hub verwendet nicht die `ProductName` Felder der obersten Ebene `CompanyName` und.

Ergreifen von Maßnahmen aufgrund der Ergebnisse in AWS Security Hub

AWS Security Hub ermöglicht es Ihnen, den aktuellen Stand Ihrer Untersuchung zu einem Ergebnis zu verfolgen.

Sie können Ergebnisse auch zur Verarbeitung an benutzerdefinierte Aktionen senden.

Themen

Den Workflow-Status von Ergebnissen festlegen

Der Workflow-Status verfolgt den Fortschritt Ihrer Untersuchung zu einem Ergebnis. Der Workflow-Status ist spezifisch für ein einzelnes Ergebnis. Er hat keinen Einfluss auf die Generierung neuer Erkenntnisse. Wenn Sie beispielsweise den Workflow-Status eines Ergebnisses auf `SUPPRESSED` oder festlegen`RESOLVED`, wird AWS Security Hub verhindert, dass für dasselbe Problem ein neues Ergebnis generiert wird.

Der Workflow-Status kann die folgenden Werte haben:

`NEW`

Der Ausgangsstatus eines Ergebnisses, bevor Sie es überprüfen.

Ergebnisse, die aus integrierten Quellen aufgenommen wurden AWS-Services AWS Config, haben z. `NEW` B. ihren ursprünglichen Status.

In den folgenden Fällen setzt Security Hub auch den Workflow-Status von entweder `NOTIFIED` oder `RESOLVED` `NEW` auf zurück:

- `RecordState` ändert sich von `ARCHIVED` in `ACTIVE`.
- `Compliance.Status`ändert sich von `PASSED` zu `FAILEDWARNING`, oder`NOT_AVAILABLE`.

Diese Änderungen bedeuten, dass zusätzliche Untersuchungen erforderlich sind.

`NOTIFIED`

Gibt an, dass Sie den Ressourceneigentümer über das Sicherheitsproblem informiert haben. Sie können diesen Status verwenden, wenn Sie nicht der Ressourceneigentümer sind und einen Eingriff von diesem benötigen, um ein Sicherheitsproblem zu beheben.

Wenn einer der folgenden Fälle eintritt, wird der Workflow-Status automatisch von `NOTIFIED` zu geändert`NEW`:

- `RecordState` ändert sich von `ARCHIVED` in `ACTIVE`.
- `Compliance.Status`ändert sich von `PASSED` zu `FAILEDWARNING`, oder`NOT_AVAILABLE`.

`SUPPRESSED`

Zeigt an, dass Sie das Ergebnis überprüft haben und nicht glauben, dass weitere Maßnahmen erforderlich sind.

Der Workflow-Status eines `SUPPRESSED` Ergebnisses `RecordState` ändert sich nicht, wenn er von `ARCHIVED` zu geändert wird`ACTIVE`.

`RESOLVED`

Das Ergebnis wurde überprüft und korrigiert und gilt nun als gelöst.

Das Ergebnis bleibt bestehen, `RESOLVED` es sei denn, einer der folgenden Fälle tritt ein:

- `RecordState` ändert sich von `ARCHIVED` in `ACTIVE`.

- `Compliance.Status`ändert sich von `PASSED` zu `FAILEDWARNING`, oder`NOT_AVAILABLE`.

  In diesen Fällen wird der Workflow-Status automatisch auf zurückgesetzt`NEW`.

  Falls dies der Fall `Compliance.Status` ist`PASSED`, setzt Security Hub den Workflow-Status automatisch auf`RESOLVED`.

Einstellung des Workflow-Status von Ergebnissen

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um den Workflow-Status eines oder mehrerer Ergebnisse festzulegen.

Informationen zur automatischen Aktualisierung des Workflow-Status bestimmter Ergebnisse finden Sie unterAutomation-Regeln.

Security Hub console

So legen Sie den Workflow-Status von Ergebnissen fest

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Gehen Sie wie folgt vor, um eine Ergebnisliste anzuzeigen:
   - Wählen Sie im Security Hub-Navigationsbereich Findings aus.
   - Wählen Sie im Security Hub-Navigationsbereich Insights aus. Wählen Sie einen Einblick aus. Wählen Sie dann in der Ergebnisliste ein Insight-Ergebnis aus.
   - Wählen Sie im Security Hub-Navigationsbereich Integrationen aus. Wählen Sie Ergebnisse für eine Integration anzeigen aus.
   - Wählen Sie im Security Hub-Navigationsbereich die Option Sicherheitsstandards aus. Wählen Sie Ergebnisse anzeigen, um eine Liste mit Kontrollen anzuzeigen. Wählen Sie dann eine Kontrolle aus, um eine Liste der Ergebnisse für diese Kontrolle anzuzeigen.
3. Aktivieren Sie in der Ergebnisliste das Kontrollkästchen für jedes Ergebnis, das Sie aktualisieren möchten.
4. Wählen Sie oben in der Liste unter Workflow-Status den Status aus.
5. Geben Sie im Dialogfeld Workflow-Status festlegen optional einen Hinweis ein, in dem der Grund für die Aktualisierung des Workflow-Status angegeben wird. Wählen Sie Status festlegen.

Security Hub API

Rufen Sie die BatchUpdateFindingsAPI auf. Geben Sie sowohl die Ergebnis-ID als auch den ARN des Produkts an, das den Befund generiert hat. Sie können diese Details abrufen, indem Sie die GetFindingsAPI aufrufen.

AWS CLI

Führen Sie den Befehl batch-update-findings aus. Geben Sie sowohl die Ergebnis-ID als auch den ARN des Produkts an, das den Befund generiert hat. Sie können diese Details abrufen, indem Sie den get-findingsBefehl ausführen.

```
batch-update-findings --finding-identifiers
 Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

Beispiel

```
aws securityhub batch-update-findings --finding-identifiers
 Id="arn:aws:securityhub:us-west-1:123456789012:subscription/
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --
workflow Status="RESOLVED"
```

Senden von Ergebnissen an eine benutzerdefinierte Aktion

Sie können AWS Security Hub benutzerdefinierte Aktionen erstellen, um Security Hub mit Amazon zu automatisieren EventBridge. Für benutzerdefinierte Aktionen lautet der Ereignistyp Security Hub Findings - Custom Action.

Weitere Informationen und detaillierte Schritte zum Erstellen benutzerdefinierter Aktionen finden Sie unter the section called “Automatisierte Reaktion und Problembehebung”.

Nachdem Sie eine benutzerdefinierte Aktion eingerichtet haben, können Sie Ergebnisse an sie senden.

Um Ergebnisse an eine benutzerdefinierte Aktion (Konsole) zu senden

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Gehen Sie wie folgt vor, um eine Ergebnisliste anzuzeigen:

- Wählen Sie im Security Hub-Navigationsbereich Findings aus.
- Wählen Sie im Security Hub-Navigationsbereich Insights aus. Wählen Sie einen Einblick aus. Wählen Sie dann in der Ergebnisliste ein Insight-Ergebnis aus.
- Wählen Sie im Security Hub-Navigationsbereich Integrationen aus. Wählen Sie Ergebnisse für eine Integration anzeigen aus.
- Wählen Sie im Security Hub-Navigationsbereich die Option Sicherheitsstandards aus. Wählen Sie Ergebnisse anzeigen, um eine Liste mit Kontrollen anzuzeigen. Wählen Sie dann den Namen des Steuerelements.

3. Aktivieren Sie in der Ergebnisliste das Kontrollkästchen für jedes Ergebnis, das an die benutzerdefinierte Aktion gesendet werden soll.

   Sie können bis zu 20 Ergebnisse gleichzeitig senden.
4. Wählen Sie für Aktionen die benutzerdefinierte Aktion aus.

AWS Format für Sicherheitssuche (ASFF)

AWS Security Hub verarbeitet, aggregiert, organisiert und priorisiert Erkenntnisse aus AWS Sicherheitsdiensten und Produktintegrationen von Drittanbietern. Security Hub verarbeitet diese Ergebnisse mithilfe eines Standardformats für Ergebnisse, dem AWS Security Finding Format (ASFF), das zeitaufwändige Datenkonvertierungen überflüssig macht. Anschließend werden aufgenommene Funde über Produkte hinweg korreliert, um die wichtigsten zu priorisieren.

Themen

AWS Syntax des Security Finding Format (ASFF)

Diese Seite bietet einen vollständigen Überblick über die JSON-Daten für ein Ergebnis im AWS Security Finding Format (ASFF). Das Format ist vom JSON-Schema abgeleitet. Wählen Sie einen verknüpften Objektnamen, um ein Beispiel für einen Befund für dieses Objekt anzuzeigen. Sie können Ihre Security Hub Hub-Ergebnisse mit den hier aufgeführten Ressourcen und Beispielen vergleichen, um Ihre Ergebnisse besser interpretieren zu können.

Eine Beschreibung der erforderlichen ASFF-Attribute finden Sie unterthe section called “Erforderliche Attribute der obersten Ebene”.

Beschreibungen der anderen ASFF-Attribute der obersten Ebene finden Sie unter. the section called “Optionale Attribute der obersten Ebene”

```
"Findings": [
    {
     "Action": {
      "ActionType": "string",
      "AwsApiCallAction": {
       "AffectedResources": {
        "string": "string"
       },
       "Api": "string",
       "CallerType": "string",
       "DomainDetails": {
        "Domain": "string"
       },
       "FirstSeen": "string",
       "LastSeen": "string",
       "RemoteIpDetails": {
        "City": {
         "CityName": "string"
        },
        "Country": {
         "CountryCode": "string",
         "CountryName": "string"
        },
        "IpAddressV4": "string",
        "Geolocation": {
         "Lat": number,
         "Lon": number
        },
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
         "Isp": "string",
         "Org": "string"
        }
       },
       "ServiceName": "string"
      },
```

```
      "DnsRequestAction": {
       "Blocked": boolean,
       "Domain": "string",
       "Protocol": "string"
      },
      "NetworkConnectionAction": {
       "Blocked": boolean,
       "ConnectionDirection": "string",
       "LocalPortDetails": {
        "Port": number,
        "PortName": "string"
       },
       "Protocol": "string",
       "RemoteIpDetails": {
        "City": {
         "CityName": "string"
        },
        "Country": {
         "CountryCode": "string",
         "CountryName": "string"
        },
        "IpAddressV4": "string",
        "Geolocation": {
         "Lat": number,
         "Lon": number
        },
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
         "Isp": "string",
         "Org": "string"
        }
       },
       "RemotePortDetails": {
        "Port": number,
        "PortName": "string"
       }
      },
      "PortProbeAction": {
       "Blocked": boolean,
       "PortProbeDetails": [{
        "LocalIpDetails": {
         "IpAddressV4": "string"
        },
```

```
        "LocalPortDetails": {
         "Port": number,
         "PortName": "string"
        },
        "RemoteIpDetails": {
         "City": {
          "CityName": "string"
         },
         "Country": {
          "CountryCode": "string",
          "CountryName": "string"
         },
         "GeoLocation": {
          "Lat": number,
          "Lon": number
         },
         "IpAddressV4": "string",
         "Organization": {
          "Asn": number,
          "AsnOrg": "string",
          "Isp": "string",
          "Org": "string"
         }
        }
       }]
      }
     },
     "AwsAccountId": "string",
     "AwsAccountName": "string",
     "CompanyName": "string",
     "Compliance": {
      "AssociatedStandards": [{
       "StandardsId": "string"
      }],
      "RelatedRequirements": ["string"],
      "SecurityControlId": "string",
      "SecurityControlParameters": [
       {
        "Name": "string",
        "Value": ["string"]
       }
     ],
      "Status": "string",
      "StatusReasons": [
```

```
      {
       "Description": "string",
       "ReasonCode": "string"
      }
     ]
    },
    "Confidence": number,
    "CreatedAt": "string",
    "Criticality": number,
    "Description": "string",
    "FindingProviderFields": {
     "Confidence": number,
     "Criticality": number,
     "RelatedFindings": [{
      "ProductArn": "string",
      "Id": "string"
     }],
     "Severity": {
      "Label": "string",
      "Normalized": number,
      "Original": "string"
     },
     "Types": ["string"]
    },
    "FirstObservedAt": "string",
    "GeneratorId": "string",
    "Id": "string",
    "LastObservedAt": "string",
    "Malware": [{
     "Name": "string",
     "Path": "string",
     "State": "string",
     "Type": "string"
    }],
    "Network": {
     "DestinationDomain": "string",
     "DestinationIpV4": "string",
     "DestinationIpV6": "string",
     "DestinationPort": number,
     "Direction": "string",
     "OpenPortRange": {
      "Begin": integer,
      "End": integer
     },
```

```
      "Protocol": "string",
      "SourceDomain": "string",
      "SourceIpV4": "string",
      "SourceIpV6": "string",
      "SourceMac": "string",
      "SourcePort": number
     },
     "NetworkPath": [{
      "ComponentId": "string",
      "ComponentType": "string",
      "Egress": {
       "Destination": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       },
       "Protocol": "string",
       "Source": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       }
      },
      "Ingress": {
       "Destination": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       },
       "Protocol": "string",
       "Source": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       }
      }
```

```
    }],
    "Note": {
     "Text": "string",
     "UpdatedAt": "string",
     "UpdatedBy": "string"
    },
    "PatchSummary": {
     "FailedCount": number,
     "Id": "string",
     "InstalledCount": number,
     "InstalledOtherCount": number,
     "InstalledPendingReboot": number,
     "InstalledRejectedCount": number,
     "MissingCount": number,
     "Operation": "string",
     "OperationEndTime": "string",
     "OperationStartTime": "string",
     "RebootOption": "string"
    },
    "Process": {
     "LaunchedAt": "string",
     "Name": "string",
     "ParentPid": number,
     "Path": "string",
     "Pid": number,
     "TerminatedAt": "string"
    },
    "ProductArn": "string",
    "ProductFields": {
     "string": "string"
    },
    "ProductName": "string",
    "RecordState": "string",
    "Region": "string",
    "RelatedFindings": [{
     "Id": "string",
     "ProductArn": "string"
    }],
    "Remediation": {
     "Recommendation": {
      "Text": "string",
      "Url": "string"
     }
    },
```

```
      "Resources": [{
       "ApplicationArn": "string",
       "ApplicationName": "string",
       "DataClassification": {
        "DetailedResultsLocation": "string",
        "Result": {
         "AdditionalOccurrences": boolean,
         "CustomDataIdentifiers": {
          "Detections": [{
           "Arn": "string",
           "Count": integer,
           "Name": "string",
           "Occurrences": {
            "Cells": [{
             "CellReference": "string",
             "Column": integer,
             "ColumnName": "string",
             "Row": integer
            }],
            "LineRanges": [{
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            }],
            "OffsetRanges": [{
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            }],
            "Pages": [{
             "LineRange": {
              "End": integer,
              "Start": integer,
              "StartColumn": integer
             },
             "OffsetRange": {
              "End": integer,
              "Start": integer,
              "StartColumn": integer
             },
             "PageNumber": integer
            }],
            "Records": [{
             "JsonPath": "string",
```

```
            "RecordIndex": integer
           }]
          }
         }],
         "TotalCount": integer
        },
        "MimeType": "string",
        "SensitiveData": [{
         "Category": "string",
         "Detections": [{
          "Count": integer,
          "Occurrences": {
           "Cells": [{
            "CellReference": "string",
            "Column": integer,
            "ColumnName": "string",
            "Row": integer
           }],
           "LineRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "OffsetRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "Pages": [{
            "LineRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
```

```
          }]
         },
         "Type": "string"
        }],
        "TotalCount": integer
       }],
       "SizeClassified": integer,
       "Status": {
        "Code": "string",
        "Reason": "string"
       }
      }
     },
     "Details": {
      "AwsAmazonMQBroker": {
       "AutoMinorVersionUpgrade": boolean,
       "BrokerArn": "string",
       "BrokerId": "string",
       "BrokerName": "string",
       "Configuration": {
        "Id": "string",
        "Revision": integer
       },
       "DeploymentMode": "string",
       "EncryptionOptions": {
        "UseAwsOwnedKey": boolean
       },
       "EngineType": "string",
       "EngineVersion": "string",
       "HostInstanceType": "string",
       "Logs": {
        "Audit": boolean,
        "AuditLogGroup": "string",
        "General": boolean,
        "GeneralLogGroup": "string"
       },
       "MaintenanceWindowStartTime": {
        "DayOfWeek": "string",
        "TimeOfDay": "string",
        "TimeZone": "string"
       },
       "PubliclyAccessible": boolean,
       "SecurityGroups": [
        "string"
```

```
        ],
        "StorageType": "string",
        "SubnetIds": [
         "string",
         "string"
        ],
        "Users": [{
         "Username": "string"
        }]
       },
       "AwsApiGatewayRestApi": {
        "ApiKeySource": "string",
        "BinaryMediaTypes": [" string"],
        "CreatedDate": "string",
        "Description": "string",
        "EndpointConfiguration": {
         "Types": ["string"]
        },
        "Id": "string",
        "MinimumCompressionSize": number,
        "Name": "string",
        "Version": "string"
       },
       "AwsApiGatewayStage": {
        "AccessLogSettings": {
         "DestinationArn": "string",
         "Format": "string"
        },
        "CacheClusterEnabled": boolean,
        "CacheClusterSize": "string",
        "CacheClusterStatus": "string",
        "CanarySettings": {
         "DeploymentId": "string",
         "PercentTraffic": number,
         "StageVariableOverrides": [{
          "string": "string"
         }],
         "UseStageCache": boolean
        },
        "ClientCertificateId": "string",
        "CreatedDate": "string",
        "DeploymentId": "string",
        "Description": "string",
        "DocumentationVersion": "string",
```

```
        "LastUpdatedDate": "string",
        "MethodSettings": [{
         "CacheDataEncrypted": boolean,
         "CachingEnabled": boolean,
         "CacheTtlInSeconds": number,
         "DataTraceEnabled": boolean,
         "HttpMethod": "string",
         "LoggingLevel": "string",
         "MetricsEnabled": boolean,
         "RequireAuthorizationForCacheControl": boolean,
         "ResourcePath": "string",
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number,
         "UnauthorizedCacheControlHeaderStrategy": "string"
        }],
        "StageName": "string",
        "TracingEnabled": boolean,
        "Variables": {
         "string": "string"
        },
        "WebAclArn": "string"
       },
       "AwsApiGatewayV2Api": {
        "ApiEndpoint": "string",
        "ApiId": "string",
        "ApiKeySelectionExpression": "string",
        "CorsConfiguration": {
         "AllowCredentials": boolean,
         "AllowHeaders": ["string"],
         "AllowMethods": ["string"],
         "AllowOrigins": ["string"],
         "ExposeHeaders": ["string"],
         "MaxAge": number
        },
        "CreatedDate": "string",
        "Description": "string",
        "Name": "string",
        "ProtocolType": "string",
        "RouteSelectionExpression": "string",
        "Version": "string"
       },
       "AwsApiGatewayV2Stage": {
        "AccessLogSettings": {
         "DestinationArn": "string",
```

```
          "Format": "string"
         },
         "ApiGatewayManaged": boolean,
         "AutoDeploy": boolean,
         "ClientCertificateId": "string",
         "CreatedDate": "string",
         "DefaultRouteSettings": {
          "DataTraceEnabled": boolean,
          "DetailedMetricsEnabled": boolean,
          "LoggingLevel": "string",
          "ThrottlingBurstLimit": number,
          "ThrottlingRateLimit": number
         },
         "DeploymentId": "string",
         "Description": "string",
         "LastDeploymentStatusMessage": "string",
         "LastUpdatedDate": "string",
         "RouteSettings": {
          "DetailedMetricsEnabled": boolean,
          "LoggingLevel": "string",
          "DataTraceEnabled": boolean,
          "ThrottlingBurstLimit": number,
          "ThrottlingRateLimit": number
         },
         "StageName": "string",
         "StageVariables": [{
          "string": "string"
         }]
        },
        "AwsAppSyncGraphQLApi": {
         "AwsAppSyncGraphQlApi": {
          "AdditionalAuthenticationProviders": [
          {
           "AuthenticationType": "string",
           "LambdaAuthorizerConfig": {
            "AuthorizerResultTtlInSeconds": integer,
            "AuthorizerUri": "string"
           }
          },
          {
           "AuthenticationType": "string"
          }
          ],
          "ApiId": "string",
```

```
          "Arn": "string",
          "AuthenticationType": "string",
          "Id": "string",
          "LogConfig": {
           "CloudWatchLogsRoleArn": "string",
           "ExcludeVerboseContent": boolean,
           "FieldLogLevel": "string"
          },
          "Name": "string",
          "XrayEnabled": boolean
         }
        },
        "AwsAthenaWorkGroup": {
         "Description": "string",
         "Name": "string",
         "WorkgroupConfiguration": {
          "ResultConfiguration": {
           "EncryptionConfiguration": {
            "EncryptionOption": "string",
            "KmsKey": "string"
           }
          }
         },
         "State": "string"
        },
        "AwsAutoScalingAutoScalingGroup": {
         "AvailabilityZones": [{
          "Value": "string"
         }],
         "CreatedTime": "string",
         "HealthCheckGracePeriod": integer,
         "HealthCheckType": "string",
         "LaunchConfigurationName": "string",
         "LoadBalancerNames": ["string"],
         "LaunchTemplate": {
                        "LaunchTemplateId": "string",
                        "LaunchTemplateName": "string",
                        "Version": "string"
                    },
         "MixedInstancesPolicy": {
          "InstancesDistribution": {
           "OnDemandAllocationStrategy": "string",
           "OnDemandBaseCapacity": number,
           "OnDemandPercentageAboveBaseCapacity": number,
```

```
          "SpotAllocationStrategy": "string",
          "SpotInstancePools": number,
          "SpotMaxPrice": "string"
         },
         "LaunchTemplate": {
          "LaunchTemplateSpecification": {
           "LaunchTemplateId": "string",
           "LaunchTemplateName": "string",
           "Version": "string"
          },
          "CapacityRebalance": boolean,
          "Overrides": [{
           "InstanceType": "string",
           "WeightedCapacity": "string"
          }]
         }
        }
       },
       "AwsAutoScalingLaunchConfiguration": {
        "AssociatePublicIpAddress": boolean,
        "BlockDeviceMappings": [{
         "DeviceName": "string",
         "Ebs": {
          "DeleteOnTermination": boolean,
          "Encrypted": boolean,
          "Iops": number,
          "SnapshotId": "string",
          "VolumeSize": number,
          "VolumeType": "string"
         },
         "NoDevice": boolean,
         "VirtualName": "string"
        }],
        "ClassicLinkVpcId": "string",
        "ClassicLinkVpcSecurityGroups": ["string"],
        "CreatedTime": "string",
        "EbsOptimized": boolean,
        "IamInstanceProfile": "string"
       },
       "ImageId": "string",
       "InstanceMonitoring": {
        "Enabled": boolean
       },
       "InstanceType": "string",
```

```
        "KernelId": "string",
        "KeyName": "string",
        "LaunchConfigurationName": "string",
        "MetadataOptions": {
         "HttpEndPoint": "string",
         "HttpPutReponseHopLimit": number,
         "HttpTokens": "string"
        },
        "PlacementTenancy": "string",
        "RamdiskId": "string",
        "SecurityGroups": ["string"],
        "SpotPrice": "string",
        "UserData": "string"
       },
       "AwsBackupBackupPlan": {
        "BackupPlan": {
         "AdvancedBackupSettings": [{
          "BackupOptions": {
           "WindowsVSS":"string"
          },
          "ResourceType":"string"
         }],
         "BackupPlanName": "string",
         "BackupPlanRule": [{
          "CompletionWindowMinutes": integer,
          "CopyActions": [{
           "DestinationBackupVaultArn": "string",
           "Lifecycle": {
            "DeleteAfterDays": integer,
            "MoveToColdStorageAfterDays": integer
           }
          }],
          "Lifecycle": {
           "DeleteAfterDays": integer
          },
          "RuleName": "string",
          "ScheduleExpression": "string",
          "StartWindowMinutes": integer,
          "TargetBackupVault": "string"
         }]
        },
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "VersionId": "string"
```

```
    },
     "AwsBackupBackupVault": {
      "AccessPolicy": {
       "Statement": [{
        "Action": ["string"],
        "Effect": "string",
        "Principal": {
         "AWS": "string"
        },
        "Resource": "string"
       }],
       "Version": "string"
      },
      "BackupVaultArn": "string",
      "BackupVaultName": "string",
      "EncryptionKeyArn": "string",
      "Notifications": {
       "BackupVaultEvents": ["string"],
       "SNSTopicArn": "string"
      }
     },
     "AwsBackupRecoveryPoint": {
      "BackupSizeInBytes": integer,
      "BackupVaultName": "string",
      "BackupVaultArn": "string",
      "CalculatedLifecycle": {
       "DeleteAt": "string",
       "MoveToColdStorageAt": "string"
      },
      "CompletionDate": "string",
      "CreatedBy": {
       "BackupPlanArn": "string",
       "BackupPlanId": "string",
       "BackupPlanVersion": "string",
       "BackupRuleId": "string"
      },
      "CreationDate": "string",
      "EncryptionKeyArn": "string",
      "IamRoleArn": "string",
      "IsEncrypted": boolean,
      "LastRestoreTime": "string",
      "Lifecycle": {
       "DeleteAfterDays": integer,
       "MoveToColdStorageAfterDays": integer
```

```
        },
        "RecoveryPointArn": "string",
        "ResourceArn": "string",
        "ResourceType": "string",
        "SourceBackupVaultArn": "string",
        "Status": "string",
        "StatusMessage": "string",
        "StorageClass": "string"
      },
      "AwsCertificateManagerCertificate": {
        "CertificateAuthorityArn": "string",
        "CreatedAt": "string",
        "DomainName": "string",
        "DomainValidationOptions": [{
          "DomainName": "string",
          "ResourceRecord": {
            "Name": "string",
            "Type": "string",
            "Value": "string"
          },
          "ValidationDomain": "string",
          "ValidationEmails": ["string"],
          "ValidationMethod": "string",
          "ValidationStatus": "string"
        }],
        "ExtendedKeyUsages": [{
          "Name": "string",
          "OId": "string"
        }],
        "FailureReason": "string",
        "ImportedAt": "string",
        "InUseBy": ["string"],
        "IssuedAt": "string",
        "Issuer": "string",
        "KeyAlgorithm": "string",
        "KeyUsages": [{
          "Name": "string"
        }],
        "NotAfter": "string",
        "NotBefore": "string",
        "Options": {
          "CertificateTransparencyLoggingPreference": "string"
        },
        "RenewalEligibility": "string",
```

```
        "RenewalSummary": {
         "DomainValidationOptions": [{
          "DomainName": "string",
          "ResourceRecord": {
           "Name": "string",
           "Type": "string",
           "Value": "string"
          },
          "ValidationDomain": "string",
          "ValidationEmails": ["string"],
          "ValidationMethod": "string",
          "ValidationStatus": "string"
         }],
         "RenewalStatus": "string",
         "RenewalStatusReason": "string",
         "UpdatedAt": "string"
        },
        "Serial": "string",
        "SignatureAlgorithm": "string",
        "Status": "string",
        "Subject": "string",
        "SubjectAlternativeNames": ["string"],
        "Type": "string"
       },
       "AwsCloudFormationStack": {
        "Capabilities": ["string"],
        "CreationTime": "string",
        "Description": "string",
        "DisableRollback": boolean,
        "DriftInformation": {
         "StackDriftStatus": "string"
        },
        "EnableTerminationProtection": boolean,
        "LastUpdatedTime": "string",
        "NotificationArns": ["string"],
        "Outputs": [{
         "Description": "string",
         "OutputKey": "string",
         "OutputValue": "string"
        }],
        "RoleArn": "string",
        "StackId": "string",
        "StackName": "string",
        "StackStatus": "string",
```

```
        "StackStatusReason": "string",
        "TimeoutInMinutes": number
       },
       "AwsCloudFrontDistribution": {
        "CacheBehaviors": {
         "Items": [{
          "ViewerProtocolPolicy": "string"
         }]
        },
        "DefaultCacheBehavior": {
         "ViewerProtocolPolicy": "string"
        },
        "DefaultRootObject": "string",
        "DomainName": "string",
        "Etag": "string",
        "LastModifiedTime": "string",
        "Logging": {
         "Bucket": "string",
         "Enabled": boolean,
         "IncludeCookies": boolean,
         "Prefix": "string"
        },
        "OriginGroups": {
         "Items": [{
          "FailoverCriteria": {
           "StatusCodes": {
            "Items": [number],
            "Quantity": number
           }
          }
         }]
        },
        "Origins": {
         "Items": [{
          "CustomOriginConfig": {
           "HttpPort": number,
           "HttpsPort": number,
           "OriginKeepaliveTimeout": number,
           "OriginProtocolPolicy": "string",
           "OriginReadTimeout": number,
           "OriginSslProtocols": {
            "Items": ["string"],
            "Quantity": number
           }
```

```
        },
        "DomainName": "string",
        "Id": "string",
        "OriginPath": "string",
        "S3OriginConfig": {
         "OriginAccessIdentity": "string"
        }
       }]
      },
      "Status": "string",
      "ViewerCertificate": {
       "AcmCertificateArn": "string",
       "Certificate": "string",
       "CertificateSource": "string",
       "CloudFrontDefaultCertificate": boolean,
       "IamCertificateId": "string",
       "MinimumProtocolVersion": "string",
       "SslSupportMethod": "string"
      },
      "WebAclId": "string"
     },
     "AwsCloudTrailTrail": {
      "CloudWatchLogsLogGroupArn": "string",
      "CloudWatchLogsRoleArn": "string",
      "HasCustomEventSelectors": boolean,
      "HomeRegion": "string",
      "IncludeGlobalServiceEvents": boolean,
      "IsMultiRegionTrail": boolean,
      "IsOrganizationTrail": boolean,
      "KmsKeyId": "string",
      "LogFileValidationEnabled": boolean,
      "Name": "string",
      "S3BucketName": "string",
      "S3KeyPrefix": "string",
      "SnsTopicArn": "string",
      "SnsTopicName": "string",
      "TrailArn": "string"
     },
     "AwsCloudWatchAlarm": {
      "ActionsEnabled": boolean,
      "AlarmActions": ["string"],
      "AlarmArn": "string",
      "AlarmConfigurationUpdatedTimestamp": "string",
      "AlarmDescription": "string",
```

```
        "AlarmName": "string",
        "ComparisonOperator": "string",
        "DatapointsToAlarm": number,
        "Dimensions": [{
         "Name": "string",
         "Value": "string"
        }],
        "EvaluateLowSampleCountPercentile": "string",
        "EvaluationPeriods": number,
        "ExtendedStatistic": "string",
        "InsufficientDataActions": ["string"],
        "MetricName": "string",
        "Namespace": "string",
        "OkActions": ["string"],
        "Period": number,
        "Statistic": "string",
        "Threshold": number,
        "ThresholdMetricId": "string",
        "TreatMissingData": "string",
        "Unit": "string"
       },
       "AwsCodeBuildProject": {
        "Artifacts": [{
         "ArtifactIdentifier": "string",
         "EncryptionDisabled": boolean,
         "Location": "string",
         "Name": "string",
         "NamespaceType": "string",
         "OverrideArtifactName": boolean,
         "Packaging": "string",
         "Path": "string",
         "Type": "string"
        }],
        "SecondaryArtifacts": [{
                    "ArtifactIdentifier": "string",
                    "Type": "string",
                    "Location": "string",
                    "Name": "string",
                    "NamespaceType": "string",
                    "Packaging": "string",
                    "Path": "string",
                    "EncryptionDisabled": boolean,
                    "OverrideArtifactName": boolean
                }],
```

```
        "EncryptionKey": "string",
        "Certificate": "string",
        "Environment": {
         "Certificate": "string",
         "EnvironmentVariables": [{
          "Name": "string",
          "Type": "string",
          "Value": "string"
         }],
         "ImagePullCredentialsType": "string",
         "PrivilegedMode": boolean,
         "RegistryCredential": {
          "Credential": "string",
          "CredentialProvider": "string"
         },
         "Type": "string"
        },
        "LogsConfig": {
         "CloudWatchLogs": {
          "GroupName": "string",
          "Status": "string",
          "StreamName": "string"
         },
         "S3Logs": {
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Status": "string"
         }
        },
        "Name": "string",
        "ServiceRole": "string",
        "Source": {
         "Type": "string",
         "Location": "string",
         "GitCloneDepth": integer
        },
        "VpcConfig": {
         "VpcId": "string",
         "Subnets": ["string"],
         "SecurityGroupIds": ["string"]
        }
       },
       "AwsDmsEndpoint": {
        "CertificateArn": "string",
```

```
        "DatabaseName": "string",
        "EndpointArn": "string",
        "EndpointIdentifier": "string",
        "EndpointType": "string",
        "EngineName": "string",
        "KmsKeyId": "string",
        "Port": integer,
        "ServerName": "string",
        "SslMode": "string",
        "Username": "string"
      },
      "AwsDmsReplicationInstance": {
        "AllocatedStorage": integer,
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "EngineVersion": "string",
        "KmsKeyId": "string",
        "MultiAZ": boolean,
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
        "ReplicationInstanceClass": "string",
        "ReplicationInstanceIdentifier": "string",
        "ReplicationSubnetGroup": {
            "ReplicationSubnetGroupIdentifier": "string"
        },
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "string"
            }
        ]
      },
      "AwsDmsReplicationTask": {
        "CdcStartPosition": "string",
        "Id": "string",
        "MigrationType": "string",
        "ReplicationInstanceArn": "string",
        "ReplicationTaskIdentifier": "string",
        "ReplicationTaskSettings": {
          "string": "string"
        },
        "SourceEndpointArn": "string",
        "TableMappings": {
          "string": "string"
        },
```

```
        "TargetEndpointArn": "string"
      },
      "AwsDynamoDbTable": {
        "AttributeDefinitions": [{
          "AttributeName": "string",
          "AttributeType": "string"
        }],
        "BillingModeSummary": {
          "BillingMode": "string",
          "LastUpdateToPayPerRequestDateTime": "string"
        },
        "CreationDateTime": "string",
        "DeletionProtectionEnabled": boolean,
        "GlobalSecondaryIndexes": [{
          "Backfilling": boolean,
          "IndexArn": "string",
          "IndexName": "string",
          "IndexSizeBytes": number,
          "IndexStatus": "string",
          "ItemCount": number,
          "KeySchema": [{
            "AttributeName": "string",
            "KeyType": "string"
          }],
          "Projection": {
            "NonKeyAttributes": ["string"],
            "ProjectionType": "string"
          },
          "ProvisionedThroughput": {
            "LastDecreaseDateTime": "string",
            "LastIncreaseDateTime": "string",
            "NumberOfDecreasesToday": number,
            "ReadCapacityUnits": number,
            "WriteCapacityUnits": number
          }
        }],
        "GlobalTableVersion": "string",
        "ItemCount": number,
        "KeySchema": [{
          "AttributeName": "string",
          "KeyType": "string"
        }],
        "LatestStreamArn": "string",
        "LatestStreamLabel": "string",
```

```
        "LocalSecondaryIndexes": [{
         "IndexArn": "string",
         "IndexName": "string",
         "KeySchema": [{
          "AttributeName": "string",
          "KeyType": "string"
         }],
         "Projection": {
          "NonKeyAttributes": ["string"],
          "ProjectionType": "string"
         }
        }],
        "ProvisionedThroughput": {
         "LastDecreaseDateTime": "string",
         "LastIncreaseDateTime": "string",
         "NumberOfDecreasesToday": number,
         "ReadCapacityUnits": number,
         "WriteCapacityUnits": number
        },
        "Replicas": [{
         "GlobalSecondaryIndexes": [{
          "IndexName": "string",
          "ProvisionedThroughputOverride": {
           "ReadCapacityUnits": number
          }
         }],
         "KmsMasterKeyId": "string",
         "ProvisionedThroughputOverride": {
          "ReadCapacityUnits": number
         },
         "RegionName": "string",
         "ReplicaStatus": "string",
         "ReplicaStatusDescription": "string"
        }],
        "RestoreSummary": {
         "RestoreDateTime": "string",
         "RestoreInProgress": boolean,
         "SourceBackupArn": "string",
         "SourceTableArn": "string"
        },
        "SseDescription": {
         "InaccessibleEncryptionDateTime": "string",
         "KmsMasterKeyArn": "string",
         "SseType": "string",
```

```
        "Status": "string"
       },
       "StreamSpecification": {
        "StreamEnabled": boolean,
        "StreamViewType": "string"
       },
       "TableId": "string",
       "TableName": "string",
       "TableSizeBytes": number,
       "TableStatus": "string"
      },
      "AwsEc2ClientVpnEndpoint": {
       "AuthenticationOptions": [
        {
         "MutualAuthentication": {
          "ClientRootCertificateChainArn": "string"
         },
         "Type": "string"
        }
       ],
       "ClientCidrBlock": "string",
       "ClientConnectOptions": {
        "Enabled": boolean
       },
       "ClientLoginBannerOptions": {
        "Enabled": boolean
       },
       "ClientVpnEndpointId": "string",
       "ConnectionLogOptions": {
        "Enabled": boolean
       },
       "Description": "string",
       "DnsServer": ["string"],
       "ServerCertificateArn": "string",
       "SecurityGroupIdSet": [
        "string"
       ],
       "SelfServicePortalUrl": "string",
       "SessionTimeoutHours": "integer",
       "SplitTunnel": boolean,
       "TransportProtocol": "string",
       "VpcId": "string",
       "VpnPort": integer
      },
```

```
      "AwsEc2Eip": {
       "AllocationId": "string",
       "AssociationId": "string",
       "Domain": "string",
       "InstanceId": "string",
       "NetworkBorderGroup": "string",
       "NetworkInterfaceId": "string",
       "NetworkInterfaceOwnerId": "string",
       "PrivateIpAddress": "string",
       "PublicIp": "string",
       "PublicIpv4Pool": "string"
      },
      "AwsEc2Instance": {
       "IamInstanceProfileArn": "string",
       "ImageId": "string",
       "IpV4Addresses": ["string"],
       "IpV6Addresses": ["string"],
       "KeyName": "string",
       "LaunchedAt": "string",
       "MetadataOptions": {
        "HttpEndpoint": "string",
        "HttpProtocolIpv6": "string",
        "HttpPutResponseHopLimit": number,
        "HttpTokens": "string",
        "InstanceMetadataTags": "string"
       },
       "Monitoring": {
        "State": "string"
       },
       "NetworkInterfaces": [{
        "NetworkInterfaceId": "string"
       }],
       "SubnetId": "string",
       "Type": "string",
       "VirtualizationType": "string",
       "VpcId": "string"
      },
      "AwsEc2LaunchTemplate": {
       "DefaultVersionNumber": "string",
       "ElasticGpuSpecifications": ["string"],
       "ElasticInferenceAccelerators": ["string"],
       "Id": "string",
       "ImageId": "string",
       "LatestVersionNumber": "string",
```

```
        "LaunchTemplateData": {
         "BlockDeviceMappings": [{
          "DeviceName": "string",
          "Ebs": {
           "DeleteonTermination": boolean,
           "Encrypted": boolean,
           "SnapshotId": "string",
           "VolumeSize": number,
           "VolumeType": "string"
          }
         }],
         "MetadataOptions": {
          "HttpTokens": "string",
          "HttpPutResponseHopLimit" : number
         },
         "Monitoring": {
          "Enabled": boolean
         },
         "NetworkInterfaces": [{
          "AssociatePublicIpAddress" : boolean
         }]
        },
        "LaunchTemplateName": "string",
        "LicenseSpecifications": ["string"],
        "SecurityGroupIds": ["string"],
        "SecurityGroups": ["string"],
        "TagSpecifications": ["string"]
       },
       "AwsEc2NetworkAcl": {
        "Associations": [{
         "NetworkAclAssociationId": "string",
         "NetworkAclId": "string",
         "SubnetId": "string"
        }],
        "Entries": [{
         "CidrBlock": "string",
         "Egress": boolean,
         "IcmpTypeCode": {
          "Code": number,
          "Type": number
         },
         "Ipv6CidrBlock": "string",
         "PortRange": {
          "From": number,
```

```
          "To": number
         },
         "Protocol": "string",
         "RuleAction": "string",
         "RuleNumber": number
        }],
        "IsDefault": boolean,
        "NetworkAclId": "string",
        "OwnerId": "string",
        "VpcId": "string"
       },
       "AwsEc2NetworkInterface": {
        "Attachment": {
         "AttachmentId": "string",
         "AttachTime": "string",
         "DeleteOnTermination": boolean,
         "DeviceIndex": number,
         "InstanceId": "string",
         "InstanceOwnerId": "string",
         "Status": "string"
        },
        "Ipv6Addresses": [{
         "Ipv6Address": "string"
        }],
        "NetworkInterfaceId": "string",
        "PrivateIpAddresses": [{
         "PrivateDnsName": "string",
         "PrivateIpAddress": "string"
        }],
        "PublicDnsName": "string",
        "PublicIp": "string",
        "SecurityGroups": [{
         "GroupId": "string",
         "GroupName": "string"
        }],
        "SourceDestCheck": boolean
       },
       "AwsEc2RouteTable": {
        "AssociationSet": [{
         "AssociationState": {
          "State": "string"
         },
         "Main": boolean,
         "RouteTableAssociationId": "string",
```

```
        "RouteTableId": "string"
       }],
       "PropogatingVgwSet": [],
       "RouteTableId": "string",
       "RouteSet": [
        {
         "DestinationCidrBlock": "string",
         "GatewayId": "string",
         "Origin": "string",
         "State": "string"
        },
        {
         "DestinationCidrBlock": "string",
         "GatewayId": "string",
         "Origin": "string",
         "State": "string"
        }
       ],
       "VpcId": "string"
      },
      "AwsEc2SecurityGroup": {
       "GroupId": "string",
       "GroupName": "string",
       "IpPermissions": [{
        "FromPort": number,
        "IpProtocol": "string",
        "IpRanges": [{
         "CidrIp": "string"
        }],
        "Ipv6Ranges": [{
         "CidrIpv6": "string"
        }],
        "PrefixListIds": [{
         "PrefixListId": "string"
        }],
        "ToPort": number,
        "UserIdGroupPairs": [{
         "GroupId": "string",
         "GroupName": "string",
         "PeeringStatus": "string",
         "UserId": "string",
         "VpcId": "string",
         "VpcPeeringConnectionId": "string"
        }]
```

```
        }],
        "IpPermissionsEgress": [{
         "FromPort": number,
         "IpProtocol": "string",
         "IpRanges": [{
          "CidrIp": "string"
         }],
         "Ipv6Ranges": [{
          "CidrIpv6": "string"
         }],
         "PrefixListIds": [{
          "PrefixListId": "string"
         }],
         "ToPort": number,
         "UserIdGroupPairs": [{
          "GroupId": "string",
          "GroupName": "string",
          "PeeringStatus": "string",
          "UserId": "string",
          "VpcId": "string",
          "VpcPeeringConnectionId": "string"
         }]
        }],
        "OwnerId": "string",
        "VpcId": "string"
       },
       "AwsEc2Subnet": {
        "AssignIpv6AddressOnCreation": boolean,
        "AvailabilityZone": "string",
        "AvailabilityZoneId": "string",
        "AvailableIpAddressCount": number,
        "CidrBlock": "string",
        "DefaultForAz": boolean,
        "Ipv6CidrBlockAssociationSet": [{
         "AssociationId": "string",
         "Ipv6CidrBlock": "string",
         "CidrBlockState": "string"
        }],
        "MapPublicIpOnLaunch": boolean,
        "OwnerId": "string",
        "State": "string",
        "SubnetArn": "string",
        "SubnetId": "string",
        "VpcId": "string"
```

```
      },
      "AwsEc2TransitGateway": {
       "AmazonSideAsn": number,
       "AssociationDefaultRouteTableId": "string",
       "AutoAcceptSharedAttachments": "string",
       "DefaultRouteTableAssociation": "string",
       "DefaultRouteTablePropagation": "string",
       "Description": "string",
       "DnsSupport": "string",
       "Id": "string",
       "MulticastSupport": "string",
       "PropagationDefaultRouteTableId": "string",
       "TransitGatewayCidrBlocks": ["string"],
       "VpnEcmpSupport": "string"
      },
      "AwsEc2Volume": {
       "Attachments": [{
        "AttachTime": "string",
        "DeleteOnTermination": boolean,
        "InstanceId": "string",
        "Status": "string"
       }],
       "CreateTime": "string",
       "DeviceName": "string",
       "Encrypted": boolean,
       "KmsKeyId": "string",
       "Size": number,
       "SnapshotId": "string",
       "Status": "string",
       "VolumeId": "string",
       "VolumeScanStatus": "string",
       "VolumeType": "string"
      },
      "AwsEc2Vpc": {
       "CidrBlockAssociationSet": [{
        "AssociationId": "string",
        "CidrBlock": "string",
        "CidrBlockState": "string"
       }],
       "DhcpOptionsId": "string",
       "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "string",
        "CidrBlockState": "string",
        "Ipv6CidrBlock": "string"
```

```
        }],
        "State": "string"
       },
       "AwsEc2VpcEndpointService": {
        "AcceptanceRequired": boolean,
        "AvailabilityZones": ["string"],
        "BaseEndpointDnsNames": ["string"],
        "ManagesVpcEndpoints": boolean,
        "GatewayLoadBalancerArns": ["string"],
        "NetworkLoadBalancerArns": ["string"],
        "PrivateDnsName": "string",
        "ServiceId": "string",
        "ServiceName": "string",
        "ServiceState": "string",
        "ServiceType": [{
         "ServiceType": "string"
        }]
       },
       "AwsEc2VpcPeeringConnection": {
        "AccepterVpcInfo": {
         "CidrBlock": "string",
         "CidrBlockSet": [{
          "CidrBlock": "string"
         }],
         "Ipv6CidrBlockSet": [{
          "Ipv6CidrBlock": "string"
         }],
         "OwnerId": "string",
         "PeeringOptions": {
          "AllowDnsResolutionFromRemoteVpc": boolean,
          "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
          "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
         },
         "Region": "string",
         "VpcId": "string"
        },
        "ExpirationTime": "string",
        "RequesterVpcInfo": {
         "CidrBlock": "string",
         "CidrBlockSet": [{
          "CidrBlock": "string"
         }],
         "Ipv6CidrBlockSet": [{
          "Ipv6CidrBlock": "string"
```

```
        }],
        "OwnerId": "string",
        "PeeringOptions": {
         "AllowDnsResolutionFromRemoteVpc": boolean,
         "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
         "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
        },
        "Region": "string",
        "VpcId": "string"
       },
       "Status": {
        "Code": "string",
        "Message": "string"
       },
       "VpcPeeringConnectionId": "string"
      },
      "AwsEc2VpnConnection": {
       "Category": "string",
       "CustomerGatewayConfiguration": "string",
       "CustomerGatewayId": "string",
       "Options": {
        "StaticRoutesOnly": boolean,
        "TunnelOptions": [{
         "DpdTimeoutSeconds": number,
         "IkeVersions": ["string"],
         "OutsideIpAddress": "string",
         "Phase1DhGroupNumbers": [number],
         "Phase1EncryptionAlgorithms": ["string"],
         "Phase1IntegrityAlgorithms": ["string"],
         "Phase1LifetimeSeconds": number,
         "Phase2DhGroupNumbers": [number],
         "Phase2EncryptionAlgorithms": ["string"],
         "Phase2IntegrityAlgorithms": ["string"],
         "Phase2LifetimeSeconds": number,
         "PreSharedKey": "string",
         "RekeyFuzzPercentage": number,
         "RekeyMarginTimeSeconds": number,
         "ReplayWindowSize": number,
         "TunnelInsideCidr": "string"
        }]
       },
       "Routes": [{
        "DestinationCidrBlock": "string",
        "State": "string"
```

```
        }],
        "State": "string",
        "TransitGatewayId": "string",
        "Type": "string",
        "VgwTelemetry": [{
         "AcceptedRouteCount": number,
         "CertificateArn": "string",
         "LastStatusChange": "string",
         "OutsideIpAddress": "string",
         "Status": "string",
         "StatusMessage": "string"
        }],
        "VpnConnectionId": "string",
        "VpnGatewayId": "string"
       },
       "AwsEcrContainerImage": {
        "Architecture": "string",
        "ImageDigest": "string",
        "ImagePublishedAt": "string",
        "ImageTags": ["string"],
        "RegistryId": "string",
        "RepositoryName": "string"
       },
       "AwsEcrRepository": {
        "Arn": "string",
        "ImageScanningConfiguration": {
         "ScanOnPush": boolean
        },
        "ImageTagMutability": "string",
        "LifecyclePolicy": {
         "LifecyclePolicyText": "string",
         "RegistryId": "string"
        },
        "RepositoryName": "string",
        "RepositoryPolicyText": "string"
       },
       "AwsEcsCluster": {
        "ActiveServicesCount": number,
        "CapacityProviders": ["string"],
        "ClusterArn": "string",
        "ClusterName": "string",
        "ClusterSettings": [{
         "Name": "string",
         "Value": "string"
```

```
        }],
        "Configuration": {
         "ExecuteCommandConfiguration": {
          "KmsKeyId": "string",
          "LogConfiguration": {
           "CloudWatchEncryptionEnabled": boolean,
           "CloudWatchLogGroupName": "string",
           "S3BucketName": "string",
           "S3EncryptionEnabled": boolean,
           "S3KeyPrefix": "string"
          },
          "Logging": "string"
         }
        },
        "DefaultCapacityProviderStrategy": [{
         "Base": number,
         "CapacityProvider": "string",
         "Weight": number
        }],
        "RegisteredContainerInstancesCount": number,
        "RunningTasksCount": number,
        "Status": "string"
       },
       "AwsEcsContainer": {
        "Image": "string",
        "MountPoints": [{
         "ContainerPath": "string",
         "SourceVolume": "string"
        }],
        "Name": "string",
        "Privileged": boolean
       },
       "AwsEcsService": {
        "CapacityProviderStrategy": [{
         "Base": number,
         "CapacityProvider": "string",
         "Weight": number
        }],
        "Cluster": "string",
        "DeploymentConfiguration": {
         "DeploymentCircuitBreaker": {
          "Enable": boolean,
          "Rollback": boolean
         },
```

```
        "MaximumPercent": number,
        "MinimumHealthyPercent": number
      },
      "DeploymentController": {
        "Type": "string"
      },
      "DesiredCount": number,
      "EnableEcsManagedTags": boolean,
      "EnableExecuteCommand": boolean,
      "HealthCheckGracePeriodSeconds": number,
      "LaunchType": "string",
      "LoadBalancers": [{
        "ContainerName": "string",
        "ContainerPort": number,
        "LoadBalancerName": "string",
        "TargetGroupArn": "string"
      }],
      "Name": "string",
      "NetworkConfiguration": {
        "AwsVpcConfiguration": {
          "AssignPublicIp": "string",
          "SecurityGroups": ["string"],
          "Subnets": ["string"]
        }
      },
      "PlacementConstraints": [{
        "Expression": "string",
        "Type": "string"
      }],
      "PlacementStrategies": [{
        "Field": "string",
        "Type": "string"
      }],
      "PlatformVersion": "string",
      "PropagateTags": "string",
      "Role": "string",
      "SchedulingStrategy": "string",
      "ServiceArn": "string",
      "ServiceName": "string",
      "ServiceRegistries": [{
        "ContainerName": "string",
        "ContainerPort": number,
        "Port": number,
        "RegistryArn": "string"
```

```
        }],
        "TaskDefinition": "string"
       },
       "AwsEcsTask": {
        "CreatedAt": "string",
        "ClusterArn": "string",
        "Group": "string",
        "StartedAt": "string",
        "StartedBy": "string",
        "TaskDefinitionArn": "string",
        "Version": number,
        "Volumes": [{
         "Name": "string",
         "Host": {
          "SourcePath": "string"
         }
        }],
        "Containers": [{
         "Image": "string",
         "MountPoints": [{
          "ContainerPath": "string",
          "SourceVolume": "string"
         }],
         "Name": "string",
         "Privileged": boolean
        }]
       },
       "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [{
         "Command": ["string"],
         "Cpu": number,
         "DependsOn": [{
          "Condition": "string",
          "ContainerName": "string"
         }],
         "DisableNetworking": boolean,
         "DnsSearchDomains": ["string"],
         "DnsServers": ["string"],
         "DockerLabels": {
          "string": "string"
         },
         "DockerSecurityOptions": ["string"],
         "EntryPoint": ["string"],
         "Environment": [{
```

```
          "Name": "string",
          "Value": "string"
        }],
        "EnvironmentFiles": [{
          "Type": "string",
          "Value": "string"
        }],
        "Essential": boolean,
        "ExtraHosts": [{
          "Hostname": "string",
          "IpAddress": "string"
        }],
        "FirelensConfiguration": {
          "Options": {
            "string": "string"
          },
          "Type": "string"
        },
        "HealthCheck": {
          "Command": ["string"],
          "Interval": number,
          "Retries": number,
          "StartPeriod": number,
          "Timeout": number
        },
        "Hostname": "string",
        "Image": "string",
        "Interactive": boolean,
        "Links": ["string"],
        "LinuxParameters": {
          "Capabilities": {
            "Add": ["string"],
            "Drop": ["string"]
          },
          "Devices": [{
            "ContainerPath": "string",
            "HostPath": "string",
            "Permissions": ["string"]
          }],
          "InitProcessEnabled": boolean,
          "MaxSwap": number,
          "SharedMemorySize": number,
          "Swappiness": number,
          "Tmpfs": [{
```

```
          "ContainerPath": "string",
          "MountOptions": ["string"],
          "Size": number
         }]
        },
        "LogConfiguration": {
         "LogDriver": "string",
         "Options": {
          "string": "string"
         },
         "SecretOptions": [{
          "Name": "string",
          "ValueFrom": "string"
         }]
        },
        "Memory": number,
        "MemoryReservation": number,
        "MountPoints": [{
         "ContainerPath": "string",
         "ReadOnly": boolean,
         "SourceVolume": "string"
        }],
        "Name": "string",
        "PortMappings": [{
         "ContainerPort": number,
         "HostPort": number,
         "Protocol": "string"
        }],
        "Privileged": boolean,
        "PseudoTerminal": boolean,
        "ReadonlyRootFilesystem": boolean,
        "RepositoryCredentials": {
         "CredentialsParameter": "string"
        },
        "ResourceRequirements": [{
         "Type": "string",
         "Value": "string"
        }],
        "Secrets": [{
         "Name": "string",
         "ValueFrom": "string"
        }],
        "StartTimeout": number,
        "StopTimeout": number,
```

```
        "SystemControls": [{
         "Namespace": "string",
         "Value": "string"
        }],
        "Ulimits": [{
         "HardLimit": number,
         "Name": "string",
         "SoftLimit": number
        }],
        "User": "string",
        "VolumesFrom": [{
         "ReadOnly": boolean,
         "SourceContainer": "string"
        }],
        "WorkingDirectory": "string"
       }],
       "Cpu": "string",
       "ExecutionRoleArn": "string",
       "Family": "string",
       "InferenceAccelerators": [{
        "DeviceName": "string",
        "DeviceType": "string"
       }],
       "IpcMode": "string",
       "Memory": "string",
       "NetworkMode": "string",
       "PidMode": "string",
       "PlacementConstraints": [{
        "Expression": "string",
        "Type": "string"
       }],
       "ProxyConfiguration": {
        "ContainerName": "string",
        "ProxyConfigurationProperties": [{
         "Name": "string",
         "Value": "string"
        }],
        "Type": "string"
       },
       "RequiresCompatibilities": ["string"],
       "Status": "string",
       "TaskRoleArn": "string",
       "Volumes": [{
        "DockerVolumeConfiguration": {
```

```
          "Autoprovision": boolean,
          "Driver": "string",
          "DriverOpts": {
           "string": "string"
          },
          "Labels": {
           "string": "string"
          },
          "Scope": "string"
         },
         "EfsVolumeConfiguration": {
          "AuthorizationConfig": {
           "AccessPointId": "string",
           "Iam": "string"
          },
          "FilesystemId": "string",
          "RootDirectory": "string",
          "TransitEncryption": "string",
          "TransitEncryptionPort": number
         },
         "Host": {
          "SourcePath": "string"
         },
         "Name": "string"
        }]
       },
       "AwsEfsAccessPoint": {
        "AccessPointId": "string",
        "Arn": "string",
        "ClientToken": "string",
        "FileSystemId": "string",
        "PosixUser": {
         "Gid": "string",
         "SecondaryGids": ["string"],
         "Uid": "string"
        },
        "RootDirectory": {
         "CreationInfo": {
          "OwnerGid": "string",
          "OwnerUid": "string",
          "Permissions": "string"
         },
         "Path": "string"
        }
```

```
      },
      "AwsEksCluster": {
       "Arn": "string",
       "CertificateAuthorityData": "string",
       "ClusterStatus": "string",
       "Endpoint": "string",
       "Logging": {
        "ClusterLogging": [{
         "Enabled": boolean,
         "Types": ["string"]
        }]
       },
       "Name": "string",
       "ResourcesVpcConfig": {
        "EndpointPublicAccess": boolean,
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       },
       "RoleArn": "string",
       "Version": "string"
      },
      "AwsElasticBeanstalkEnvironment": {
       "ApplicationName": "string",
       "Cname": "string",
       "DateCreated": "string",
       "DateUpdated": "string",
       "Description": "string",
       "EndpointUrl": "string",
       "EnvironmentArn": "string",
       "EnvironmentId": "string",
       "EnvironmentLinks": [{
        "EnvironmentName": "string",
        "LinkName": "string"
       }],
       "EnvironmentName": "string",
       "OptionSettings": [{
        "Namespace": "string",
        "OptionName": "string",
        "ResourceName": "string",
        "Value": "string"
       }],
       "PlatformArn": "string",
       "SolutionStackName": "string",
       "Status": "string",
```

```
        "Tier": {
         "Name": "string",
         "Type": "string",
         "Version": "string"
        },
        "VersionLabel": "string"
       },
       "AwsElasticSearchDomain": {
        "AccessPolicies": "string",
        "DomainStatus": {
         "DomainId": "string",
         "DomainName": "string",
         "Endpoint": "string",
         "Endpoints": {
          "string": "string"
         }
        },
        "DomainEndpointOptions": {
         "EnforceHTTPS": boolean,
         "TLSSecurityPolicy": "string"
        },
        "ElasticsearchClusterConfig": {
         "DedicatedMasterCount": number,
         "DedicatedMasterEnabled": boolean,
         "DedicatedMasterType": "string",
         "InstanceCount": number,
         "InstanceType": "string",
         "ZoneAwarenessConfig": {
          "AvailabilityZoneCount": number
         },
         "ZoneAwarenessEnabled": boolean
        },
        "ElasticsearchVersion": "string",
        "EncryptionAtRestOptions": {
         "Enabled": boolean,
         "KmsKeyId": "string"
        },
        "LogPublishingOptions": {
         "AuditLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "IndexSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
```

```
          "Enabled": boolean
         },
         "SearchSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         }
        },
        "NodeToNodeEncryptionOptions": {
         "Enabled": boolean
        },
        "ServiceSoftwareOptions": {
         "AutomatedUpdateDate": "string",
         "Cancellable": boolean,
         "CurrentVersion": "string",
         "Description": "string",
         "NewVersion": "string",
         "UpdateAvailable": boolean,
         "UpdateStatus": "string"
        },
        "VPCOptions": {
         "AvailabilityZones": [
          "string"
         ],
         "SecurityGroupIds": [
          "string"
         ],
         "SubnetIds": [
          "string"
         ],
         "VPCId": "string"
        }
       },
       "AwsElbLoadBalancer": {
        "AvailabilityZones": ["string"],
        "BackendServerDescriptions": [{
         "InstancePort": number,
         "PolicyNames": ["string"]
        }],
        "CanonicalHostedZoneName": "string",
        "CanonicalHostedZoneNameID": "string",
        "CreatedTime": "string",
        "DnsName": "string",
        "HealthCheck": {
         "HealthyThreshold": number,
```

```
        "Interval": number,
        "Target": "string",
        "Timeout": number,
        "UnhealthyThreshold": number
       },
       "Instances": [{
        "InstanceId": "string"
       }],
       "ListenerDescriptions": [{
        "Listener": {
         "InstancePort": number,
         "InstanceProtocol": "string",
         "LoadBalancerPort": number,
         "Protocol": "string",
         "SslCertificateId": "string"
        },
        "PolicyNames": ["string"]
       }],
       "LoadBalancerAttributes": {
        "AccessLog": {
         "EmitInterval": number,
         "Enabled": boolean,
         "S3BucketName": "string",
         "S3BucketPrefix": "string"
        },
        "ConnectionDraining": {
         "Enabled": boolean,
         "Timeout": number
        },
        "ConnectionSettings": {
         "IdleTimeout": number
        },
        "CrossZoneLoadBalancing": {
         "Enabled": boolean
        },
        "AdditionalAttributes": [{
                        "Key": "string",
                        "Value": "string"
                    }]
       },
       "LoadBalancerName": "string",
       "Policies": {
        "AppCookieStickinessPolicies": [{
         "CookieName": "string",
```

```
          "PolicyName": "string"
         }],
         "LbCookieStickinessPolicies": [{
          "CookieExpirationPeriod": number,
          "PolicyName": "string"
         }],
         "OtherPolicies": ["string"]
        },
        "Scheme": "string",
        "SecurityGroups": ["string"],
        "SourceSecurityGroup": {
         "GroupName": "string",
         "OwnerAlias": "string"
        },
        "Subnets": ["string"],
        "VpcId": "string"
       },
       "AwsElbv2LoadBalancer": {
        "AvailabilityZones": {
         "SubnetId": "string",
         "ZoneName": "string"
        },
        "CanonicalHostedZoneId": "string",
        "CreatedTime": "string",
        "DNSName": "string",
        "IpAddressType": "string",
        "LoadBalancerAttributes": [{
         "Key": "string",
         "Value": "string"
        }],
        "Scheme": "string",
        "SecurityGroups": ["string"],
        "State": {
         "Code": "string",
         "Reason": "string"
        },
        "Type": "string",
        "VpcId": "string"
       },
       "AwsEventSchemasRegistry": {
        "Description": "string",
        "RegistryArn": "string",
        "RegistryName": "string"
       },
```

```
      "AwsEventsEndpoint": {
       "Arn": "string",
       "Description": "string",
       "EndpointId": "string",
       "EndpointUrl": "string",
       "EventBuses": [
           {
               "EventBusArn": "string"
           },
           {
               "EventBusArn": "string"
           }
       ],
       "Name": "string",
       "ReplicationConfig": {
           "State": "string"
       },
       "RoleArn": "string",
       "RoutingConfig": {
           "FailoverConfig": {
               "Primary": {
                   "HealthCheck": "string"
               },
               "Secondary": {
                   "Route": "string"
               }
           }
       },
       "State": "string"
      },
      "AwsEventsEventBus": {
       "Arn": "string",
       "Name": "string",
       "Policy": "string"
      },
      "AwsGuardDutyDetector": {
       "FindingPublishingFrequency": "string",
       "ServiceRole": "string",
       "Status": "string",
       "DataSources": {
        "CloudTrail": {
         "Status": "string"
        },
        "DnsLogs": {
```

```
          "Status": "string"
         },
         "FlowLogs": {
          "Status": "string"
         },
         "S3Logs": {
          "Status": "string"
         },
         "Kubernetes": {
          "AuditLogs": {
           "Status": "string"
          }
         },
         "MalwareProtection": {
          "ScanEc2InstanceWithFindings": {
           "EbsVolumes": {
            "Status": "string"
           }
          },
          "ServiceRole": "string"
         }
        }
       },
       "AwsIamAccessKey": {
        "AccessKeyId": "string",
        "AccountId": "string",
        "CreatedAt": "string",
        "PrincipalId": "string",
        "PrincipalName": "string",
        "PrincipalType": "string",
        "SessionContext": {
         "Attributes": {
          "CreationDate": "string",
          "MfaAuthenticated": boolean
         },
         "SessionIssuer": {
          "AccountId": "string",
          "Arn": "string",
          "PrincipalId": "string",
          "Type": "string",
          "UserName": "string"
         }
        },
        "Status": "string"
```

```
      },
      "AwsIamGroup": {
       "AttachedManagedPolicies": [{
        "PolicyArn": "string",
        "PolicyName": "string"
       }],
       "CreateDate": "string",
       "GroupId": "string",
       "GroupName": "string",
       "GroupPolicyList": [{
        "PolicyName": "string"
       }],
       "Path": "string"
      },
      "AwsIamPolicy": {
       "AttachmentCount": number,
       "CreateDate": "string",
       "DefaultVersionId": "string",
       "Description": "string",
       "IsAttachable": boolean,
       "Path": "string",
       "PermissionsBoundaryUsageCount": number,
       "PolicyId": "string",
       "PolicyName": "string",
       "PolicyVersionList": [{
        "CreateDate": "string",
        "IsDefaultVersion": boolean,
        "VersionId": "string"
       }],
       "UpdateDate": "string"
      },
      "AwsIamRole": {
       "AssumeRolePolicyDocument": "string",
       "AttachedManagedPolicies": [{
        "PolicyArn": "string",
        "PolicyName": "string"
       }],
       "CreateDate": "string",
       "InstanceProfileList": [{
        "Arn": "string",
        "CreateDate": "string",
        "InstanceProfileId": "string",
        "InstanceProfileName": "string",
        "Path": "string",
```

```
        "Roles": [{
         "Arn": "string",
         "AssumeRolePolicyDocument": "string",
         "CreateDate": "string",
         "Path": "string",
         "RoleId": "string",
         "RoleName": "string"
        }]
       }],
       "MaxSessionDuration": number,
       "Path": "string",
       "PermissionsBoundary": {
        "PermissionsBoundaryArn": "string",
        "PermissionsBoundaryType": "string"
       },
       "RoleId": "string",
       "RoleName": "string",
       "RolePolicyList": [{
        "PolicyName": "string"
       }]
      },
      "AwsIamUser": {
       "AttachedManagedPolicies": [{
        "PolicyArn": "string",
        "PolicyName": "string"
       }],
       "CreateDate": "string",
       "GroupList": ["string"],
       "Path": "string",
       "PermissionsBoundary": {
        "PermissionsBoundaryArn": "string",
        "PermissionsBoundaryType": "string"
       },
       "UserId": "string",
       "UserName": "string",
       "UserPolicyList": [{
        "PolicyName": "string"
       }]
      },
      "AwsKinesisStream": {
       "Arn": "string",
       "Name": "string",
       "RetentionPeriodHours": number,
       "ShardCount": number,
```

```
        "StreamEncryption": {
         "EncryptionType": "string",
         "KeyId": "string"
        }
       },
       "AwsKmsKey": {
        "AWSAccountId": "string",
        "CreationDate": "string",
        "Description": "string",
        "KeyId": "string",
        "KeyManager": "string",
        "KeyRotationStatus": boolean,
        "KeyState": "string",
        "Origin": "string"
       },
       "AwsLambdaFunction": {
        "Architectures": [
         "string"
        ],
        "Code": {
         "S3Bucket": "string",
         "S3Key": "string",
         "S3ObjectVersion": "string",
         "ZipFile": "string"
        },
        "CodeSha256": "string",
        "DeadLetterConfig": {
         "TargetArn": "string"
        },
        "Environment": {
         "Variables": {
          "Stage": "string"
         },
         "Error": {
          "ErrorCode": "string",
          "Message": "string"
         }
        },
        "FunctionName": "string",
        "Handler": "string",
        "KmsKeyArn": "string",
        "LastModified": "string",
        "Layers": {
         "Arn": "string",
```

```
        "CodeSize": number
       },
       "PackageType": "string",
       "RevisionId": "string",
       "Role": "string",
       "Runtime": "string",
       "Timeout": integer,
       "TracingConfig": {
        "Mode": "string"
       },
       "Version": "string",
       "VpcConfig": {
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       },
       "MasterArn": "string",
       "MemorySize": number
      },
      "AwsLambdaLayerVersion": {
       "CompatibleRuntimes": [
        "string"
       ],
       "CreatedDate": "string",
       "Version": number
      },
      "AwsMskCluster": {
       "ClusterInfo": {
        "ClientAuthentication": {
         "Sasl": {
          "Scram": {
           "Enabled": boolean
          },
          "Iam": {
           "Enabled": boolean
          }
         },
         "Tls": {
          "CertificateAuthorityArnList": [],
          "Enabled": boolean
         },
         "Unauthenticated": {
          "Enabled": boolean
         }
        },
```

```
        "ClusterName": "string",
        "CurrentVersion": "string",
        "EncryptionInfo": {
         "EncryptionAtRest": {
          "DataVolumeKMSKeyId": "string"
         },
         "EncryptionInTransit": {
          "ClientBroker": "string",
          "InCluster": boolean
         }
        },
        "EnhancedMonitoring": "string",
        "NumberOfBrokerNodes": integer
       }
      },
      "AwsNetworkFirewallFirewall": {
       "DeleteProtection": boolean,
       "Description": "string",
       "FirewallArn": "string",
       "FirewallId": "string",
       "FirewallName": "string",
       "FirewallPolicyArn": "string",
       "FirewallPolicyChangeProtection": boolean,
       "SubnetChangeProtection": boolean,
       "SubnetMappings": [{
        "SubnetId": "string"
       }],
       "VpcId": "string"
      },
      "AwsNetworkFirewallFirewallPolicy": {
       "Description": "string",
       "FirewallPolicy": {
        "StatefulRuleGroupReferences": [{
         "ResourceArn": "string"
        }],
        "StatelessCustomActions": [{
         "ActionDefinition": {
          "PublishMetricAction": {
           "Dimensions": [{
            "Value": "string"
           }]
          }
         },
         "ActionName": "string"
```

```
        }],
        "StatelessDefaultActions": ["string"],
        "StatelessFragmentDefaultActions": ["string"],
        "StatelessRuleGroupReferences": [{
         "Priority": number,
         "ResourceArn": "string"
        }]
       },
       "FirewallPolicyArn": "string",
       "FirewallPolicyId": "string",
       "FirewallPolicyName": "string"
      },
      "AwsNetworkFirewallRuleGroup": {
       "Capacity": number,
       "Description": "string",
       "RuleGroup": {
        "RulesSource": {
         "RulesSourceList": {
          "GeneratedRulesType": "string",
          "Targets": ["string"],
          "TargetTypes": ["string"]
         },
         "RulesString": "string",
         "StatefulRules": [{
          "Action": "string",
          "Header": {
           "Destination": "string",
           "DestinationPort": "string",
           "Direction": "string",
           "Protocol": "string",
           "Source": "string",
           "SourcePort": "string"
          },
          "RuleOptions": [{
           "Keyword": "string",
           "Settings": ["string"]
          }]
         }],
         "StatelessRulesAndCustomActions": {
          "CustomActions": [{
           "ActionDefinition": {
            "PublishMetricAction": {
             "Dimensions": [{
              "Value": "string"
```

```
            }]
           }
          },
          "ActionName": "string"
         }],
         "StatelessRules": [{
          "Priority": number,
          "RuleDefinition": {
           "Actions": ["string"],
           "MatchAttributes": {
            "DestinationPorts": [{
             "FromPort": number,
             "ToPort": number
            }],
            "Destinations": [{
             "AddressDefinition": "string"
            }],
            "Protocols": [number],
            "SourcePorts": [{
             "FromPort": number,
             "ToPort": number
            }],
            "Sources": [{
             "AddressDefinition": "string"
            }],
            "TcpFlags": [{
             "Flags": ["string"],
             "Masks": ["string"]
            }]
           }
          }
         }]
        }
       },
       "RuleVariables": {
        "IpSets": {
         "Definition": ["string"]
        },
        "PortSets": {
         "Definition": ["string"]
        }
       }
      },
      "RuleGroupArn": "string",
```

```
        "RuleGroupId": "string",
        "RuleGroupName": "string",
        "Type": "string"
       },
       "AwsOpenSearchServiceDomain": {
        "AccessPolicies": "string",
        "AdvancedSecurityOptions": {
         "Enabled": boolean,
         "InternalUserDatabaseEnabled": boolean,
         "MasterUserOptions": {
          "MasterUserArn": "string",
          "MasterUserName": "string",
          "MasterUserPassword": "string"
         }
        },
        "Arn": "string",
        "ClusterConfig": {
         "DedicatedMasterCount": number,
         "DedicatedMasterEnabled": boolean,
         "DedicatedMasterType": "string",
         "InstanceCount": number,
         "InstanceType": "string",
         "WarmCount": number,
         "WarmEnabled": boolean,
         "WarmType": "string",
         "ZoneAwarenessConfig": {
          "AvailabilityZoneCount": number
         },
         "ZoneAwarenessEnabled": boolean
        },
        "DomainEndpoint": "string",
        "DomainEndpointOptions": {
         "CustomEndpoint": "string",
         "CustomEndpointCertificateArn": "string",
         "CustomEndpointEnabled": boolean,
         "EnforceHTTPS": boolean,
         "TLSSecurityPolicy": "string"
        },
        "DomainEndpoints": {
         "string": "string"
        },
        "DomainName": "string",
        "EncryptionAtRestOptions": {
         "Enabled": boolean,
```

```
        "KmsKeyId": "string"
       },
       "EngineVersion": "string",
       "Id": "string",
       "LogPublishingOptions": {
        "AuditLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        },
        "IndexSlowLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        },
        "SearchSlowLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        }
       },
       "NodeToNodeEncryptionOptions": {
        "Enabled": boolean
       },
       "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "string",
        "Cancellable": boolean,
        "CurrentVersion": "string",
        "Description": "string",
        "NewVersion": "string",
        "OptionalDeployment": boolean,
        "UpdateAvailable": boolean,
        "UpdateStatus": "string"
       },
       "VpcOptions": {
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       }
      },
      "AwsRdsDbCluster": {
       "ActivityStreamStatus": "string",
       "AllocatedStorage": number,
       "AssociatedRoles": [{
        "RoleArn": "string",
        "Status": "string"
       }],
       "AutoMinorVersionUpgrade": boolean,
```

```
        "AvailabilityZones": ["string"],
        "BackupRetentionPeriod": integer,
        "ClusterCreateTime": "string",
        "CopyTagsToSnapshot": boolean,
        "CrossAccountClone": boolean,
        "CustomEndpoints": ["string"],
        "DatabaseName": "string",
        "DbClusterIdentifier": "string",
        "DbClusterMembers": [{
         "DbClusterParameterGroupStatus": "string",
         "DbInstanceIdentifier": "string",
         "IsClusterWriter": boolean,
         "PromotionTier": integer
        }],
        "DbClusterOptionGroupMemberships": [{
         "DbClusterOptionGroupName": "string",
         "Status": "string"
        }],
        "DbClusterParameterGroup": "string",
        "DbClusterResourceId": "string",
        "DbSubnetGroup": "string",
        "DeletionProtection": boolean,
        "DomainMemberships": [{
         "Domain": "string",
         "Fqdn": "string",
         "IamRoleName": "string",
         "Status": "string"
        }],
        "EnabledCloudwatchLogsExports": ["string"],
        "Endpoint": "string",
        "Engine": "string",
        "EngineMode": "string",
        "EngineVersion": "string",
        "HostedZoneId": "string",
        "HttpEndpointEnabled": boolean,
        "IamDatabaseAuthenticationEnabled": boolean,
        "KmsKeyId": "string",
        "MasterUsername": "string",
        "MultiAz": boolean,
        "Port": integer,
        "PreferredBackupWindow": "string",
        "PreferredMaintenanceWindow": "string",
        "ReaderEndpoint": "string",
        "ReadReplicaIdentifiers": ["string"],
```

```
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcSecurityGroups": [{
         "Status": "string",
         "VpcSecurityGroupId": "string"
        }]
       },
       "AwsRdsDbClusterSnapshot": {
        "AllocatedStorage": integer,
        "AvailabilityZones": ["string"],
        "ClusterCreateTime": "string",
        "DbClusterIdentifier": "string",
        "DbClusterSnapshotAttributes": [{
         "AttributeName": "string",
         "AttributeValues": ["string"]
        }],
        "DbClusterSnapshotIdentifier": "string",
        "Engine": "string",
        "EngineVersion": "string",
        "IamDatabaseAuthenticationEnabled": boolean,
        "KmsKeyId": "string",
        "LicenseModel": "string",
        "MasterUsername": "string",
        "PercentProgress": integer,
        "Port": integer,
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcId": "string"
       },
       "AwsRdsDbInstance": {
        "AllocatedStorage": number,
        "AssociatedRoles": [{
         "RoleArn": "string",
         "FeatureName": "string",
         "Status": "string"
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "BackupRetentionPeriod": number,
        "CACertificateIdentifier": "string",
        "CharacterSetName": "string",
        "CopyTagsToSnapshot": boolean,
```

```
        "DBClusterIdentifier": "string",
        "DBInstanceClass": "string",
        "DBInstanceIdentifier": "string",
        "DbInstancePort": number,
        "DbInstanceStatus": "string",
        "DbiResourceId": "string",
        "DBName": "string",
        "DbParameterGroups": [{
         "DbParameterGroupName": "string",
         "ParameterApplyStatus": "string"
        }],
        "DbSecurityGroups": ["string"],
        "DbSubnetGroup": {
         "DbSubnetGroupArn": "string",
         "DbSubnetGroupDescription": "string",
         "DbSubnetGroupName": "string",
         "SubnetGroupStatus": "string",
         "Subnets": [{
          "SubnetAvailabilityZone": {
           "Name": "string"
          },
          "SubnetIdentifier": "string",
          "SubnetStatus": "string"
         }],
         "VpcId": "string"
        },
        "DeletionProtection": boolean,
        "Endpoint": {
         "Address": "string",
         "Port": number,
         "HostedZoneId": "string"
        },
        "DomainMemberships": [{
         "Domain": "string",
         "Fqdn": "string",
         "IamRoleName": "string",
         "Status": "string"
        }],
        "EnabledCloudwatchLogsExports": ["string"],
        "Engine": "string",
        "EngineVersion": "string",
        "EnhancedMonitoringResourceArn": "string",
        "IAMDatabaseAuthenticationEnabled": boolean,
        "InstanceCreateTime": "string",
```

```
        "Iops": number,
        "KmsKeyId": "string",
        "LatestRestorableTime": "string",
        "LicenseModel": "string",
        "ListenerEndpoint": {
         "Address": "string",
         "HostedZoneId": "string",
         "Port": number
        },
        "MasterUsername": "admin",
        "MaxAllocatedStorage": number,
        "MonitoringInterval": number,
        "MonitoringRoleArn": "string",
        "MultiAz": boolean,
        "OptionGroupMemberships": [{
         "OptionGroupName": "string",
         "Status": "string"
        }],
        "PendingModifiedValues": {
         "AllocatedStorage": number,
         "BackupRetentionPeriod": number,
         "CaCertificateIdentifier": "string",
         "DbInstanceClass": "string",
         "DbInstanceIdentifier": "string",
         "DbSubnetGroupName": "string",
         "EngineVersion": "string",
         "Iops": number,
         "LicenseModel": "string",
         "MasterUserPassword": "string",
         "MultiAZ": boolean,
         "PendingCloudWatchLogsExports": {
          "LogTypesToDisable": ["string"],
          "LogTypesToEnable": ["string"]
         },
         "Port": number,
         "ProcessorFeatures": [{
          "Name": "string",
          "Value": "string"
         }],
         "StorageType": "string"
        },
        "PerformanceInsightsEnabled": boolean,
        "PerformanceInsightsKmsKeyId": "string",
        "PerformanceInsightsRetentionPeriod": number,
```

```
        "PreferredBackupWindow": "string",
        "PreferredMaintenanceWindow": "string",
        "ProcessorFeatures": [{
         "Name": "string",
         "Value": "string"
        }],
        "PromotionTier": number,
        "PubliclyAccessible": boolean,
        "ReadReplicaDBClusterIdentifiers": ["string"],
        "ReadReplicaDBInstanceIdentifiers": ["string"],
        "ReadReplicaSourceDBInstanceIdentifier": "string",
        "SecondaryAvailabilityZone": "string",
        "StatusInfos": [{
         "Message": "string",
         "Normal": boolean,
         "Status": "string",
         "StatusType": "string"
        }],
        "StorageEncrypted": boolean,
        "TdeCredentialArn": "string",
        "Timezone": "string",
        "VpcSecurityGroups": [{
         "VpcSecurityGroupId": "string",
         "Status": "string"
        }]
       },
       "AwsRdsDbSecurityGroup": {
        "DbSecurityGroupArn": "string",
        "DbSecurityGroupDescription": "string",
        "DbSecurityGroupName": "string",
        "Ec2SecurityGroups": [{
         "Ec2SecurityGroupuId": "string",
         "Ec2SecurityGroupName": "string",
         "Ec2SecurityGroupOwnerId": "string",
         "Status": "string"
        }],
        "IpRanges": [{
         "CidrIp": "string",
         "Status": "string"
        }],
        "OwnerId": "string",
        "VpcId": "string"
       },
       "AwsRdsDbSnapshot": {
```

```
        "AllocatedStorage": integer,
        "AvailabilityZone": "string",
        "DbInstanceIdentifier": "string",
        "DbiResourceId": "string",
        "DbSnapshotIdentifier": "string",
        "Encrypted": boolean,
        "Engine": "string",
        "EngineVersion": "string",
        "IamDatabaseAuthenticationEnabled": boolean,
        "InstanceCreateTime": "string",
        "Iops": number,
        "KmsKeyId": "string",
        "LicenseModel": "string",
        "MasterUsername": "string",
        "OptionGroupName": "string",
        "PercentProgress": integer,
        "Port": integer,
        "ProcessorFeatures": [],
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "SourceDbSnapshotIdentifier": "string",
        "SourceRegion": "string",
        "Status": "string",
        "StorageType": "string",
        "TdeCredentialArn": "string",
        "Timezone": "string",
        "VpcId": "string"
      },
      "AwsRdsEventSubscription": {
        "CustomerAwsId": "string",
        "CustSubscriptionId": "string",
        "Enabled": boolean,
        "EventCategoriesList": ["string"],
        "EventSubscriptionArn": "string",
        "SnsTopicArn": "string",
        "SourceIdsList": ["string"],
        "SourceType": "string",
        "Status": "string",
        "SubscriptionCreationTime": "string"
      },
      "AwsRedshiftCluster": {
        "AllowVersionUpgrade": boolean,
        "AutomatedSnapshotRetentionPeriod": number,
        "AvailabilityZone": "string",
```

```
        "ClusterAvailabilityStatus": "string",
        "ClusterCreateTime": "string",
        "ClusterIdentifier": "string",
        "ClusterNodes": [{
         "NodeRole": "string",
         "PrivateIPAddress": "string",
         "PublicIPAddress": "string"
        }],
        "ClusterParameterGroups": [{
         "ClusterParameterStatusList": [{
          "ParameterApplyErrorDescription": "string",
          "ParameterApplyStatus": "string",
          "ParameterName": "string"
         }],
         "ParameterApplyStatus": "string",
         "ParameterGroupName": "string"
        }],
        "ClusterPublicKey": "string",
        "ClusterRevisionNumber": "string",
        "ClusterSecurityGroups": [{
         "ClusterSecurityGroupName": "string",
         "Status": "string"
        }],
        "ClusterSnapshotCopyStatus": {
         "DestinationRegion": "string",
         "ManualSnapshotRetentionPeriod": number,
         "RetentionPeriod": number,
         "SnapshotCopyGrantName": "string"
        },
        "ClusterStatus": "string",
        "ClusterSubnetGroupName": "string",
        "ClusterVersion": "string",
        "DBName": "string",
        "DeferredMaintenanceWindows": [{
         "DeferMaintenanceEndTime": "string",
         "DeferMaintenanceIdentifier": "string",
         "DeferMaintenanceStartTime": "string"
        }],
        "ElasticIpStatus": {
         "ElasticIp": "string",
         "Status": "string"
        },
        "ElasticResizeNumberOfNodeOptions": "string",
        "Encrypted": boolean,
```

```
        "Endpoint": {
         "Address": "string",
         "Port": number
        },
        "EnhancedVpcRouting": boolean,
        "ExpectedNextSnapshotScheduleTime": "string",
        "ExpectedNextSnapshotScheduleTimeStatus": "string",
        "HsmStatus": {
         "HsmClientCertificateIdentifier": "string",
         "HsmConfigurationIdentifier": "string",
         "Status": "string"
        },
        "IamRoles": [{
         "ApplyStatus": "string",
         "IamRoleArn": "string"
        }],
        "KmsKeyId": "string",
        "LoggingStatus":{
                    "BucketName": "string",
                    "LastFailureMessage": "string",
                    "LastFailureTime": "string",
                    "LastSuccessfulDeliveryTime": "string",
                    "LoggingEnabled": boolean,
                    "S3KeyPrefix": "string"
                },
        "MaintenanceTrackName": "string",
        "ManualSnapshotRetentionPeriod": number,
        "MasterUsername": "string",
        "NextMaintenanceWindowStartTime": "string",
        "NodeType": "string",
        "NumberOfNodes": number,
        "PendingActions": ["string"],
        "PendingModifiedValues": {
         "AutomatedSnapshotRetentionPeriod": number,
         "ClusterIdentifier": "string",
         "ClusterType": "string",
         "ClusterVersion": "string",
         "EncryptionType": "string",
         "EnhancedVpcRouting": boolean,
         "MaintenanceTrackName": "string",
         "MasterUserPassword": "string",
         "NodeType": "string",
         "NumberOfNodes": number,
         "PubliclyAccessible": "string"
```

```
        },
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
        "ResizeInfo": {
         "AllowCancelResize": boolean,
         "ResizeType": "string"
        },
        "RestoreStatus": {
         "CurrentRestoreRateInMegaBytesPerSecond": number,
         "ElapsedTimeInSeconds": number,
         "EstimatedTimeToCompletionInSeconds": number,
         "ProgressInMegaBytes": number,
         "SnapshotSizeInMegaBytes": number,
         "Status": "string"
        },
        "SnapshotScheduleIdentifier": "string",
        "SnapshotScheduleState": "string",
        "VpcId": "string",
        "VpcSecurityGroups": [{
         "Status": "string",
         "VpcSecurityGroupId": "string"
        }]
       },
       "AwsRoute53HostedZone": {
        "HostedZone": {
         "Id": "string",
         "Name": "string",
         "Config": {
          "Comment": "string"
         }
        },
        "NameServers": ["string"],
        "QueryLoggingConfig": {
         "CloudWatchLogsLogGroupArn": {
          "CloudWatchLogsLogGroupArn": "string",
          "Id": "string",
          "HostedZoneId": "string"
         }
        },
        "Vpcs": [
         {
          "Id": "string",
          "Region": "string"
         }
```

```
        ]
       },
       "AwsS3AccessPoint": {
        "AccessPointArn": "string",
        "Alias": "string",
        "Bucket": "string",
        "BucketAccountId": "string",
        "Name": "string",
        "NetworkOrigin": "string",
        "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": boolean,
         "BlockPublicPolicy": boolean,
         "IgnorePublicAcls": boolean,
         "RestrictPublicBuckets": boolean
        },
        "VpcConfiguration": {
         "VpcId": "string"
        }
       },
       "AwsS3AccountPublicAccessBlock": {
        "BlockPublicAcls": boolean,
        "BlockPublicPolicy": boolean,
        "IgnorePublicAcls": boolean,
        "RestrictPublicBuckets": boolean
       },
       "AwsS3Bucket": {
        "AccessControlList": "string",
        "BucketLifecycleConfiguration": {
         "Rules": [{
          "AbortIncompleteMultipartUpload": {
           "DaysAfterInitiation": number
          },
          "ExpirationDate": "string",
          "ExpirationInDays": number,
          "ExpiredObjectDeleteMarker": boolean,
          "Filter": {
           "Predicate": {
            "Operands": [{
              "Prefix": "string",
              "Type": "string"
             },
             {
              "Tag": {
               "Key": "string",
```

```
            "Value": "string"
           },
           "Type": "string"
          }
         ],
         "Type": "string"
        }
       },
       "Id": "string",
       "NoncurrentVersionExpirationInDays": number,
       "NoncurrentVersionTransitions": [{
        "Days": number,
        "StorageClass": "string"
       }],
       "Prefix": "string",
       "Status": "string",
       "Transitions": [{
        "Date": "string",
        "Days": number,
        "StorageClass": "string"
       }]
      }]
     },
     "BucketLoggingConfiguration": {
      "DestinationBucketName": "string",
      "LogFilePrefix": "string"
     },
     "BucketName": "string",
     "BucketNotificationConfiguration": {
      "Configurations": [{
       "Destination": "string",
       "Events": ["string"],
       "Filter": {
        "S3KeyFilter": {
         "FilterRules": [{
          "Name": "string",
          "Value": "string"
         }]
        }
       },
       "Type": "string"
      }]
     },
     "BucketVersioningConfiguration": {
```

```
        "IsMfaDeleteEnabled": boolean,
        "Status": "string"
       },
       "BucketWebsiteConfiguration": {
        "ErrorDocument": "string",
        "IndexDocumentSuffix": "string",
        "RedirectAllRequestsTo": {
         "HostName": "string",
         "Protocol": "string"
        },
        "RoutingRules": [{
         "Condition": {
          "HttpErrorCodeReturnedEquals": "string",
          "KeyPrefixEquals": "string"
         },
         "Redirect": {
          "HostName": "string",
          "HttpRedirectCode": "string",
          "Protocol": "string",
          "ReplaceKeyPrefixWith": "string",
          "ReplaceKeyWith": "string"
         }
        }]
       },
       "CreatedAt": "string",
       "ObjectLockConfiguration": {
        "ObjectLockEnabled": "string",
        "Rule": {
         "DefaultRetention": {
          "Days": integer,
          "Mode": "string",
          "Years": integer
         }
        }
       },
       "OwnerAccountId": "string",
       "OwnerId": "string",
       "OwnerName": "string",
       "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": boolean,
        "BlockPublicPolicy": boolean,
        "IgnorePublicAcls": boolean,
        "RestrictPublicBuckets": boolean
       },
```

```
        "ServerSideEncryptionConfiguration": {
         "Rules": [{
          "ApplyServerSideEncryptionByDefault": {
           "KMSMasterKeyID": "string",
           "SSEAlgorithm": "string"
          }
         }]
        }
       },
       "AwsS3Object": {
        "ContentType": "string",
        "ETag": "string",
        "LastModified": "string",
        "ServerSideEncryption": "string",
        "SSEKMSKeyId": "string",
        "VersionId": "string"
       },
       "AwsSagemakerNotebookInstance": {
        "DirectInternetAccess": "string",
        "InstanceMetadataServiceConfiguration": {
         "MinimumInstanceMetadataServiceVersion": "string"
        },
        "InstanceType": "string",
        "LastModifiedTime": "string",
        "NetworkInterfaceId": "string",
        "NotebookInstanceArn": "string",
        "NotebookInstanceName": "string",
        "NotebookInstanceStatus": "string",
        "PlatformIdentifier": "string",
        "RoleArn": "string",
        "RootAccess": "string",
        "SecurityGroups": ["string"],
        "SubnetId": "string",
        "Url": "string",
        "VolumeSizeInGB": number
       },
       "AwsSecretsManagerSecret": {
        "Deleted": boolean,
        "Description": "string",
        "KmsKeyId": "string",
        "Name": "string",
        "RotationEnabled": boolean,
        "RotationLambdaArn": "string",
        "RotationOccurredWithinFrequency": boolean,
```

```
        "RotationRules": {
         "AutomaticallyAfterDays": integer
        }
       },
       "AwsSnsTopic": {
        "ApplicationSuccessFeedbackRoleArn": "string",
        "FirehoseFailureFeedbackRoleArn": "string",
        "FirehoseSuccessFeedbackRoleArn": "string",
        "HttpFailureFeedbackRoleArn": "string",
        "HttpSuccessFeedbackRoleArn": "string",
        "KmsMasterKeyId": "string",
        "Owner": "string",
        "SqsFailureFeedbackRoleArn": "string",
        "SqsSuccessFeedbackRoleArn": "string",
        "Subscription": {
         "Endpoint": "string",
         "Protocol": "string"
        },
        "TopicName": "string"
       },
       "AwsSqsQueue": {
        "DeadLetterTargetArn": "string",
        "KmsDataKeyReusePeriodSeconds": number,
        "KmsMasterKeyId": "string",
        "QueueName": "string"
       },
       "AwsSsmPatchCompliance": {
        "Patch": {
         "ComplianceSummary": {
          "ComplianceType": "string",
          "CompliantCriticalCount": integer,
          "CompliantHighCount": integer,
          "CompliantInformationalCount": integer,
          "CompliantLowCount": integer,
          "CompliantMediumCount": integer,
          "CompliantUnspecifiedCount": integer,
          "ExecutionType": "string",
          "NonCompliantCriticalCount": integer,
          "NonCompliantHighCount": integer,
          "NonCompliantInformationalCount": integer,
          "NonCompliantLowCount": integer,
          "NonCompliantMediumCount": integer,
          "NonCompliantUnspecifiedCount": integer,
          "OverallSeverity": "string",
```

```
          "PatchBaselineId": "string",
          "PatchGroup": "string",
          "Status": "string"
         }
        }
       },
       "AwsStepFunctionStateMachine": {
        "StateMachineArn": "string",
        "Name": "string",
        "Status": "string",
        "RoleArn": "string",
        "Type": "string",
        "LoggingConfiguration": {
         "Level": "string",
         "IncludeExecutionData": boolean
        },
        "TracingConfiguration": {
         "Enabled": boolean
        }
       },
       "AwsWafRateBasedRule": {
        "MatchPredicates": [{
         "DataId": "string",
         "Negated": boolean,
         "Type": "string"
        }],
        "MetricName": "string",
        "Name": "string",
        "RateKey": "string",
        "RateLimit": number,
        "RuleId": "string"
       },
       "AwsWafRegionalRateBasedRule": {
        "MatchPredicates": [{
         "DataId": "string",
         "Negated": boolean,
         "Type": "string"
        }],
        "MetricName": "string",
        "Name": "string",
        "RateKey": "string",
        "RateLimit": number,
        "RuleId": "string"
       },
```

```
      "AwsWafRegionalRule": {
       "MetricName": "string",
       "Name": "string",
       "RuleId": "string",
       "PredicateList": [{
           "DataId": "string",
           "Negated": boolean,
           "Type": "string"
       }]
      },
      "AwsWafRegionalRuleGroup": {
       "MetricName": "string",
       "Name": "string",
       "RuleGroupId": "string",
       "Rules": [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }]
      },
      "AwsWafRegionalWebAcl": {
       "DefaultAction": "string",
       "MetricName" : "string",
       "Name": "string",
       "RulesList" : [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string",
        "ExcludedRules": [{
         "ExclusionType": "string",
         "RuleId": "string"
        }],
        "OverrideAction": {
         "Type": "string"
        }
       }],
       "WebAclId": "string"
      },
```

```
      "AwsWafRule": {
       "MetricName": "string",
       "Name": "string",
       "PredicateList": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
       }],
       "RuleId": "string"
      },
      "AwsWafRuleGroup": {
       "MetricName": "string",
       "Name": "string",
       "RuleGroupId": "string",
       "Rules": [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }]
      },
      "AwsWafv2RuleGroup": {
       "Arn": "string",
       "Capacity": number,
       "Description": "string",
       "Id": "string",
       "Name": "string",
       "Rules": [{
        "Action": {
        "Allow": {
         "CustomRequestHandling": {
          "InsertHeaders": [
           {
           "Name": "string",
           "Value": "string"
           },
           {
           "Name": "string",
           "Value": "string"
           }
          ]
         }
```

```
        }
        },
        "Name": "string",
        "Priority": number,
        "VisibilityConfig": {
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string",
         "SampledRequestsEnabled": boolean
        }
       }],
       "VisibilityConfig": {
        "CloudWatchMetricsEnabled": boolean,
        "MetricName": "string",
        "SampledRequestsEnabled": boolean
       }
      },
      "AwsWafWebAcl": {
       "DefaultAction": "string",
       "Name": "string",
       "Rules": [{
        "Action": {
         "Type": "string"
        },
        "ExcludedRules": [{
         "RuleId": "string"
        }],
        "OverrideAction": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }],
       "WebAclId": "string"
      },
      "AwsWafv2WebAcl": {
       "Arn": "string",
       "Capacity": number,
       "CaptchaConfig": {
        "ImmunityTimeProperty": {
         "ImmunityTime": number
        }
       },
       "DefaultAction": {
```

```
        "Block": {}
       },
       "Description": "string",
       "ManagedbyFirewallManager": boolean,
       "Name": "string",
       "Rules": [{
        "Action": {
         "RuleAction": {
          "Block": {}
         }
        },
        "Name": "string",
        "Priority": number,
        "VisibilityConfig": {
         "SampledRequestsEnabled": boolean,
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string"
        }
       }],
       "VisibilityConfig": {
        "SampledRequestsEnabled": boolean,
        "CloudWatchMetricsEnabled": boolean,
        "MetricName": "string"
       }
      },
      "AwsXrayEncryptionConfig": {
       "KeyId": "string",
       "Status": "string",
       "Type": "string"
      },
      "Container": {
       "ContainerRuntime": "string",
       "ImageId": "string",
       "ImageName": "string",
       "LaunchedAt": "string",
       "Name": "string",
       "Privileged": boolean,
       "VolumeMounts": [{
        "Name": "string",
        "MountPath": "string"
       }]
      },
      "Other": {
       "string": "string"
```

```
      },
      "Id": "string",
      "Partition": "string",
      "Region": "string",
      "ResourceRole": "string",
      "Tags": {
       "string": "string"
      },
      "Type": "string"
     }],
     "SchemaVersion": "string",
     "Severity": {
      "Label": "string",
      "Normalized": number,
      "Original": "string"
     },
     "Sample": boolean,
     "SourceUrl": "string",
     "Threats": [{
      "FilePaths": [{
       "FileName": "string",
       "FilePath": "string",
       "Hash": "string",
       "ResourceId": "string"
      }],
      "ItemCount": number,
      "Name": "string",
      "Severity": "string"
     }],
     "ThreatIntelIndicators": [{
      "Category": "string",
      "LastObservedAt": "string",
      "Source": "string",
      "SourceUrl": "string",
      "Type": "string",
      "Value": "string"
     }],
     "Title": "string",
     "Types": ["string"],
     "UpdatedAt": "string",
     "UserDefinedFields": {
      "string": "string"
     },
     "VerificationState": "string",
```

```
      "Vulnerabilities": [{
       "CodeVulnerabilities": [{
        "Cwes": [
         "string",
         "string"
        ],
        "FilePath": {
         "EndLine": integer,
         "FileName": "string",
         "FilePath": "string",
         "StartLine": integer
        },
        "SourceArn":"string"
       }],
       "Cvss": [{
        "Adjustments": [{
         "Metric": "string",
         "Reason": "string"
        }],
        "BaseScore": number,
        "BaseVector": "string",
        "Source": "string",
        "Version": "string"
       }],
       "EpssScore": number,
       "ExploitAvailable": "string",
       "FixAvailable": "string",
       "Id": "string",
       "LastKnownExploitAt": "string",
       "ReferenceUrls": ["string"],
       "RelatedVulnerabilities": ["string"],
       "Vendor": {
        "Name": "string",
        "Url": "string",
        "VendorCreatedAt": "string",
        "VendorSeverity": "string",
        "VendorUpdatedAt": "string"
       },
       "VulnerablePackages": [{
        "Architecture": "string",
        "Epoch": "string",
        "FilePath": "string",
        "FixedInVersion": "string",
        "Name": "string",
```

```
        "PackageManager": "string",
        "Release": "string",
        "Remediation": "string",
        "SourceLayerArn": "string",
        "SourceLayerHash": "string",
        "Version": "string"
       }]
      }],
      "Workflow": {
       "Status": "string"
      },
      "WorkflowState": "string"
     }
]
```

Auswirkungen der Konsolidierung auf ASFF-Felder und -Werte

Security Hub bietet zwei Arten der Konsolidierung:

- Ansicht konsolidierter Kontrollen (immer aktiviert; kann nicht ausgeschaltet werden) — Jedes Steuerelement hat standardübergreifend eine einzige Kennung. Auf der Seite „Kontrollen“ der Security Hub Hub-Konsole werden all Ihre Kontrollen standardübergreifend angezeigt.
- Konsolidierte Kontrollbefunde (können ein- oder ausgeschaltet werden) — Wenn konsolidierte Kontrollbefunde aktiviert sind, generiert Security Hub ein einziges Ergebnis für eine Sicherheitsüberprüfung, auch wenn eine Prüfung über mehrere Standards hinweg gemeinsam genutzt wird. Dadurch soll das Auffinden von Geräuschen reduziert werden. Consolidated Control Findings ist standardmäßig für Sie aktiviert, wenn Sie Security Hub am oder nach dem 23. Februar 2023 aktiviert haben. Andernfalls ist es standardmäßig ausgeschaltet. Konsolidierte Kontrollergebnisse sind in Security Hub Hub-Mitgliedskonten jedoch nur aktiviert, wenn sie im Administratorkonto aktiviert sind. Wenn die Funktion im Administratorkonto deaktiviert ist, ist sie auch in den Mitgliedskonten deaktiviert. Anweisungen zum Aktivieren dieser Funktion finden Sie unterDie konsolidierten Kontrollergebnisse werden aktiviert.

Beide Funktionen beinhalten Änderungen an der Steuerung der Suche nach Feldern und Werten in derAWS Format für Sicherheitssuche (ASFF). In diesem Abschnitt werden diese Änderungen zusammengefasst.

Ansicht der konsolidierten Kontrollen — ASFF-Änderungen

Mit der Funktion zur Ansicht konsolidierter Kontrollen wurden die folgenden Änderungen an den Feldern und Werten für die Kontrollsuche in der ASFF eingeführt.

Wenn Ihre Workflows nicht auf den Werten dieser Kontrollfelder basieren, sind keine Maßnahmen erforderlich.

Wenn Sie Workflows haben, die auf den spezifischen Werten dieser Kontrollfindungsfelder basieren, aktualisieren Sie Ihre Workflows, sodass sie die aktuellen Werte verwenden.

ASFF-Feld	Beispielwert vor Ansicht der konsolidierten Kontrollen	Beispielwert nach Ansicht der konsolidierten Kontrollen sowie Beschreibung der Änderung
Einhaltung der Vorschriften. SecurityControlId	Nicht zutreffend (neues Feld)	EC2.2 Führt eine einzige Kontroll-ID für alle Standards ein. `ProductFields.RuleId` stellt weiterhin die standardbasierte Kontroll-ID für CIS v1.2.0-Steuerelemente bereit. `ProductFields.ControlId` stellt immer noch die standardbasierte Kontroll-ID für Steuerungen in anderen Standards bereit.

ASFF-Feld	Beispielwert vor Ansicht der konsolidierten Kontrollen	Beispielwert nach Ansicht der konsolidierten Kontrollen sowie Beschreibung der Änderung
Einhaltung der Vorschriften. AssociatedStandards	Nicht zutreffend (neues Feld)	[{“ StandardsId „: „Standards/ aws-foundational-security-best -practices/v/1.0.0 "}] Zeigt an, in welchen Standards ein Steuerelement aktiviert ist.
ProductFields. ArchivalReasons. ----SEP----:0/ Beschreibung	Nicht zutreffend (neues Feld)	„Das Ergebnis befindet sich im Status ARCHIVIERT, da konsolidierte Kontrollergebnisse aktiviert oder deaktiviert wurden. Dies führt dazu, dass Ergebnisse im vorherigen Status archiviert werden, wenn neue Ergebnisse generiert werden.“ Beschreibt, warum Security Hub bestehende Ergebnisse archiviert hat.

ASFF-Feld	Beispielwert vor Ansicht der konsolidierten Kontrollen	Beispielwert nach Ansicht der konsolidierten Kontrollen sowie Beschreibung der Änderung
ProductFields. ArchivalReasons. ----sep----:0/ReasonCode	Nicht zutreffend (neues Feld)	„CONSOLIDATED_CONTROL_FINDINGS_UPDATE“ Gibt den Grund an, warum Security Hub bestehende Ergebnisse archiviert hat.
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Dieses Feld verweist nicht mehr auf einen Standard.
Abhilfe.Empfehlung.Text	„Anweisungen zur Behebung dieses Problems finden Sie in der AWS Security Hub PCI DSS-Dokumentation.“	„Anweisungen zur Behebung dieses Problems finden Sie in der Dokumentation zu den AWS Security Hub-Steuerungen.“ Dieses Feld verweist nicht mehr auf einen Standard.

ASFF-Feld	Beispielwert vor Ansicht der konsolidierten Kontrollen	Beispielwert nach Ansicht der konsolidierten Kontrollen sowie Beschreibung der Änderung
Abhilfe.Empfehlung.Url	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Dieses Feld verweist nicht mehr auf einen Standard.

Konsolidierte Kontrollergebnisse — ASFF-Änderungen

Wenn Sie die Option „Konsolidierte Kontrollergebnisse“ aktivieren, können sich die folgenden Änderungen an den Feldern und Werten der Kontrollergebnisse in der ASFF auf Sie auswirken. Diese Änderungen kommen zu den Änderungen hinzu, die zuvor für die Ansicht konsolidierter Kontrollen beschrieben wurden.

Wenn Ihre Workflows nicht auf den Werten dieser Kontrollfindungsfelder basieren, sind keine Maßnahmen erforderlich.

Wenn Sie Workflows haben, die auf den spezifischen Werten dieser Kontrollfindungsfelder basieren, aktualisieren Sie Ihre Workflows, sodass sie die aktuellen Werte verwenden.

> **Note**
>
> Automated Security Response auf AWS Version 2.0.0 unterstützt konsolidierte Kontrollergebnisse. Wenn Sie diese Version der Lösung verwenden, können Sie Ihre Workflows beibehalten, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

ASFF-Feld	Beispielwert vor der Aktivierung konsolidierter Kontrollergebnisse	Beispielwert nach dem Einschalten der konsolidierten Kontrollergebnisse und Beschreibung der Änderung
GeneratorId	aws-foundational-security-best-Praktiken/V/1.0.0/Config.1	Sicherheitskontrolle/Config.1 Dieses Feld verweist nicht mehr auf einen Standard.
Title	AWS Config PCI.Config.1 sollte aktiviert sein	AWS Config sollte aktiviert sein Dieses Feld verweist nicht mehr auf standardspezifische Informationen.
Id	arn:aws:securityhub:eu-central-1:123456789012:subscription/pci-dss/v/3.2.1/pci.iam.5/finding/ab6d6a26-a156-48f0-9403-115983e5a956	arn:aws:securityhub:eu-central-1:123456789012:sicherheitskontrolle/iam.9/finding/ab6d6a26-a156-48f0-9403-115983e5a956 Dieses Feld verweist nicht mehr auf einen Standard.
ProductFields.ControlId	PCI.EC2.2	Entfernt. Siehe `Compliance.SecurityControlId` stattdessen. Dieses Feld wurde zugunsten einer einzigen, standardunabhängigen Kontroll-ID entfernt.
ProductFields.RuleId	1.3	Entfernt. Siehe `Compliance.SecurityControlId` stattdessen.

ASFF-Feld	Beispielwert vor der Aktivierung konsolidierter Kontrollergebnisse	Beispielwert nach dem Einschalten der konsolidierten Kontrollergebnisse und Beschreibung der Änderung
		Dieses Feld wurde zugunsten einer einzigen, standardunabhängigen Kontroll-ID entfernt.
Beschreibung	Diese PCI-DSS-Steuerung prüft, ob sie im Girokonto und in der Region aktiviert AWS Config ist.	Diese AWS Kontrolle prüft, ob sie im Girokonto und in der Region aktiviert AWS Config ist. Dieses Feld verweist nicht mehr auf einen Standard.

Schweregrad	„Schweregrad“: {
	
	„Produkt“: 90,
	
	„Label“: „KRITISCH“,
	
	„Normalisiert“: 90,
	
	„Original“: „KRITISCH“
	
	}
		„Schweregrad“: {
		
		„Label“: „KRITISCH“,
		
		„Normalisiert“: 90,
		
		„Original“: „KRITISCH“
		
		}
		
		Security Hub verwendet das Feld Produkt nicht mehr, um den Schweregrad eines Fehlers zu beschreiben.

Typen	["Software- und Konfigurationsprüfungen/Branchen- und behördliche Standards/PCI-DSS"]	["Software- und Konfigurationsprüfungen/Branchen- und Regulierungsstandards"] Dieses Feld verweist nicht mehr auf einen Standard.

ASFF-Feld	Beispielwert vor der Aktivierung konsolidierter Kontrollergebnisse	Beispielwert nach dem Einschalten der konsolidierten Kontrollergebnisse und Beschreibung der Änderung
Einhaltung. RelatedRequirements	["PCI DSS 10.5.2“, „PCI DSS 11.5", „CIS AWS Foundations 2.5"]	["PCI DSS v3.2.1/10.5.2“, „PCI DSS v3.2.1/11,5“, „Benchmark v1.2.0/2.5" der CIS Foundations] AWS In diesem Feld werden die entsprechenden Anforderungen in allen aktivierten Standards angezeigt.
CreatedAt	2015-05-05T 08:18:13.138 Z	25.09.2022 08:18:13,138 Z Das Format bleibt unverändert, aber der Wert wird zurückgesetzt, wenn Sie die Option „Konsolidierte Kontrollergebnisse“ aktivieren.
FirstObservedAt	2021-05-07T 08:18:13.138 Z	28.09.2022 08:18:13.138 Z Das Format bleibt unverändert, aber der Wert wird zurückgesetzt, wenn Sie die Option „Konsolidierte Kontrollergebnisse“ aktivieren.
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation	Entfernt. Siehe `Remediation.Recommendation.Url` stattdessen.

ASFF-Feld	Beispielwert vor der Aktivierung konsolidierter Kontrollergebnisse	Beispielwert nach dem Einschalten der konsolidierten Kontrollergebnisse und Beschreibung der Änderung
ProductFields.StandardsArn	arn:aws:securityhub: ::standards/ -practices/v/1.0.0 aws-foundational-security-best	Entfernt. Siehe `Compliance.AssociatedStandards` stattdessen.
ProductFields.StandardsControlArn	arn:aws:securityhub:us-east-1:123456789012:control/ -practices/v/1.0.0/config.1 aws-foundational-security-best	Entfernt. Security Hub generiert ein Ergebnis für eine standardübergreifende Sicherheitsüberprüfung.
ProductFields.StandardsGuideArn	arn:aws:securityhub: ::ruleset/ /v/1.2.0 cis-aws-foundations-benchmark	Entfernt. Siehe `Compliance.AssociatedStandards` stattdessen.
ProductFields.StandardsGuideSubscriptionArn	arn:aws:securityhub:us-east-2:123456789012:subscription/ /v/1.2.0 cis-aws-foundations-benchmark	Entfernt. Security Hub generiert ein Ergebnis für eine standardübergreifende Sicherheitsüberprüfung.
ProductFields.StandardsSubscriptionArn	arn:aws:securityhub:us-east-1:123456789012:subscription/ -practices/v/1.0.0 aws-foundational-security-best	Entfernt. Security Hub generiert ein Ergebnis für eine standardübergreifende Sicherheitsüberprüfung.
ProductFields.aws/securityhub/ FindingId	arn:aws:securityhub:us-east-1: :product/aws/securityhub/ arn:aws:securityhub:us-east-1:123456789012:subscrition/ -practices/v/1.0.0/config.1/finding/751c2173-7372-4e12-8656-a5210dfb1d67 aws-foundational-security-best	arn:aws:securityhub:us-east-1: :product/aws/securityhub/ arn:aws:securityhub:us-east-1:123456789012:sicherheitskontrolle/config.1/finding/751c2173-7372-4e12-8656-A5210dfb1d67 Dieses Feld verweist nicht mehr auf einen Standard.

Werte für vom Kunden bereitgestellte ASFF-Felder nach Aktivierung der konsolidierten Kontrollergebnisse

Wenn Sie konsolidierte Kontrollergebnisse aktivieren, generiert Security Hub ein standardübergreifendes Ergebnis und archiviert die ursprünglichen Ergebnisse (separate Ergebnisse für jeden Standard). Um archivierte Ergebnisse anzuzeigen, können Sie die Seite Ergebnisse der Security Hub Hub-Konsole aufrufen, wobei der Filter Datensatzstatus auf ARCHIVIERT gesetzt ist, oder die `GetFindings`API-Aktion verwenden. Aktualisierungen, die Sie an den ursprünglichen Ergebnissen in der Security Hub Hub-Konsole oder mithilfe der BatchUpdateFindingsAPI vorgenommen haben, werden in den neuen Ergebnissen nicht beibehalten (bei Bedarf können Sie diese Daten wiederherstellen, indem Sie auf die archivierten Ergebnisse verweisen).

Vom Kunden bereitgestelltes ASFF-Feld	Beschreibung der Änderung nach der Aktivierung der konsolidierten Kontrollergebnisse
Wahrscheinlichkeit	Wird auf den leeren Zustand zurückgesetzt.
Kritikalität	Setzt auf den leeren Zustand zurück.
Hinweis	Setzt auf den leeren Zustand zurück.
RelatedFindings	Setzt auf den leeren Zustand zurück.
Schweregrad	Standardschweregrad des Ergebnisses (entspricht dem Schweregrad der Kontrolle).
Typen	Wird auf den standardunabhängigen Wert zurückgesetzt.
UserDefinedFields	Setzt auf den leeren Zustand zurück.
VerificationState	Setzt auf den leeren Zustand zurück.
Workflow	Neue fehlgeschlagene Ergebnisse haben den Standardwert. `NEW` Neue bestandene Ergebnisse haben einen Standardwert von`RESOLVED`.

Generator-IDs vor und nach dem Einschalten konsolidierter Kontrollergebnisse

Im Folgenden finden Sie eine Liste der Änderungen der Generator-ID für Kontrollen, wenn Sie konsolidierte Kontrollergebnisse aktivieren. Diese gelten für Kontrollen, die Security Hub am 15. Februar 2023 unterstützt hat.

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.1 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudWatch .1
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.10 cis-aws-foundations-benchmark	Sicherheitskontrolle/IAM.16
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.11 cis-aws-foundations-benchmark	Sicherheitskontrolle/IAM.17
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.12 cis-aws-foundations-benchmark	Sicherheitskontrolle/IAM.4
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.13 cis-aws-foundations-benchmark	Sicherheitskontrolle/IAM.9
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.14 cis-aws-foundations-benchmark	Sicherheitskontrolle/IAM.6
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.16 cis-aws-foundations-benchmark	Sicherheitskontrolle/IAM.2
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.2 cis-aws-foundations-benchmark	Sicherheitskontrolle/IAM.5
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.20 cis-aws-foundations-benchmark	Sicherheitskontrolle/IAM.18
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.22 cis-aws-foundations-benchmark	Sicherheitskontrolle/IAM.1

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.3 cis-aws-foundations-benchmark	Sicherheitskontrolle/IAM.8
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.4 cis-aws-foundations-benchmark	Sicherheitskontrolle/IAM.3
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.5 cis-aws-foundations-benchmark	Sicherheitskontrolle/IAM.11
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.6 cis-aws-foundations-benchmark	Sicherheitskontrolle/IAM.12
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.7 cis-aws-foundations-benchmark	Sicherheitskontrolle/IAM.13
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.8 cis-aws-foundations-benchmark	Sicherheitskontrolle/IAM.14
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.9 cis-aws-foundations-benchmark	Sicherheitskontrolle/IAM.15
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.1 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudTrail .1
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.2 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudTrail .4
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.3 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudTrail .6
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.4 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudTrail .5
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.5 cis-aws-foundations-benchmark	Sicherheitskontrolle/Config.1

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.6 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudTrail .7
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.7 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudTrail .2
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.8 cis-aws-foundations-benchmark	Sicherheitskontrolle/KMS.4
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.9 cis-aws-foundations-benchmark	Sicherheitskontrolle/EC2.6
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.1 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudWatch .2
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.2 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudWatch .3
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.3 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudWatch .1
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.4 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudWatch .4
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.5 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudWatch .5
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.6 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudWatch .6
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.7 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudWatch .7
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.8 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudWatch .8

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.9 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudWatch .9
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.10 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudWatch .10
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.11 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudWatch .11
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.12 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudWatch .12
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.13 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudWatch .13
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.14 cis-aws-foundations-benchmark	Sicherheitskontrolle/ CloudWatch .14
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/4.1 cis-aws-foundations-benchmark	Sicherheitskontrolle/EC2.13
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/4.2 cis-aws-foundations-benchmark	Sicherheitskontrolle/EC2.14
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/4.3 cis-aws-foundations-benchmark	Sicherheitskontrolle/EC2.2
cis-aws-foundations-benchmark/v/1.4.0/1.10	Sicherheitskontrolle/IAM.5
cis-aws-foundations-benchmark/v/1.4.0/1.14	Sicherheitskontrolle/IAM.3
cis-aws-foundations-benchmark/v/1.4.0/1.16	Sicherheitskontrolle/IAM.1
cis-aws-foundations-benchmark/v/1.4.0/1.17	Sicherheitskontrolle/IAM.18
cis-aws-foundations-benchmark/v/1.4.0/1.4	Sicherheitskontrolle/IAM.4

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
cis-aws-foundations-benchmark/v/1.4.0/1.5	Sicherheitskontrolle/IAM.9
cis-aws-foundations-benchmark/v/1.4.0/1.6	Sicherheitskontrolle/IAM.6
cis-aws-foundations-benchmark/v/1.4.0/1.7	Sicherheitskontrolle/ 1. CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/1.8	Sicherheitskontrolle/IAM.15
cis-aws-foundations-benchmark/v/1.4.0/1.9	Sicherheitskontrolle/IAM.16
cis-aws-foundations-benchmark/v/1.4.0/2.1.2	Sicherheitskontrolle/S3.5
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.1	Sicherheitskontrolle/S3.1
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.2	Sicherheitskontrolle/S3.8
cis-aws-foundations-benchmark/v/1.4.0/2.2.1	Sicherheitskontrolle/EC2.7
cis-aws-foundations-benchmark/v/1.4.0/2.3.1	Sicherheitskontrolle/RDS.3
cis-aws-foundations-benchmark/v/1.4.0/3.1	Sicherheitskontrolle/ 1. CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.2	Sicherheitskontrolle/ .4 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.4	Sicherheitskontrolle/ .5 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.5	Sicherheitskontrolle/Config.1
cis-aws-foundations-benchmark/v/1.4.0/3.6	Sicherheitskontrolle/S3.9
cis-aws-foundations-benchmark/v/1.4.0/3.7	Sicherheitskontrolle/ .2 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.8	Sicherheitskontrolle/KMS.4
cis-aws-foundations-benchmark/v/1.4.0/3.9	Sicherheitskontrolle/EC2.6
cis-aws-foundations-benchmark/v/1.4.0/4.3	Sicherheitskontrolle/ 1. CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.4	Sicherheitskontrolle/ .4 CloudWatch

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
cis-aws-foundations-benchmark/v/1.4.0/4.5	Sicherheitskontrolle/ 4.5 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.6	Sicherheitskontrolle/ .6 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.7	Sicherheitskontrolle/ .7 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.8	Sicherheitskontrolle/ .8 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.9	Sicherheitskontrolle/ .9 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.10	Sicherheitskontrolle/ 1.0 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.11	Sicherheitskontrolle/ 1.1 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4,12	Sicherheitskontrolle/ 1.2 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.13	Sicherheitskontrolle/ 1.3 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.14	Sicherheitskontrolle/ 1.4 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/5.1	Sicherheitskontrolle/EC2.21
cis-aws-foundations-benchmark/v/1.4.0/5.3	Sicherheitskontrolle/EC2.2
aws-foundational-security-best-Praktiken/V/1.0.0/Account.1	Sicherheitskontrolle/Account.1
aws-foundational-security-best-Praktiken/V/1.0.0/ACM.1	Sicherheitskontrolle/ACM.1
aws-foundational-security-best-Praktiken / V/1.0.0/APIGateway.1	Sicherheitskontrolle/APIGateway.1
aws-foundational-security-best-Praktiken / V/1.0.0/APIGateway.2	Sicherheitskontrolle/APIGateway.2
aws-foundational-security-best-Praktiken / V/1.0.0/APIGateway.3	Sicherheitskontrolle/APIGateway.3

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
aws-foundational-security-best-Praktiken / V/1.0.0/APIGateway.4	Sicherheitskontrolle/APIGateway.4
aws-foundational-security-best-Praktiken / V/1.0.0/APIGateway.5	Sicherheitskontrolle/APIGateway.5
aws-foundational-security-best-Praktiken / V/1.0.0/APIGateway.8	Sicherheitskontrolle/APIGateway.8
aws-foundational-security-best-Praktiken / V/1.0.0/APIGateway.9	Sicherheitskontrolle/APIGateway.9
aws-foundational-security-best-Praktiken / v/1.0.0/ 1. AutoScaling	Sicherheitskontrolle/ .1 AutoScaling
aws-foundational-security-best-Praktiken/v/1.0.0/ AutoScaling .2	Sicherheitskontrolle/ .2 AutoScaling
aws-foundational-security-best-praktiken/v/1.0.0/ AutoScaling .3	Sicherheitskontrolle/ .3 AutoScaling
aws-foundational-security-best-Praktiken/V/1.0.0/AutoScaling.5	Sicherheitskontrolle/Autoscaling.5
aws-foundational-security-best-Praktiken/v/1.0.0/ .6 AutoScaling	Sicherheitskontrolle/ .6 AutoScaling
aws-foundational-security-best-praktiken/v/1.0.0/ AutoScaling .9	Sicherheitskontrolle/ .9 AutoScaling
aws-foundational-security-best-Praktiken/v/1.0.0/ CloudFront .1	Sicherheitskontrolle/ .1 CloudFront
aws-foundational-security-best-Praktiken/v/1.0.0/ CloudFront .3	Sicherheitskontrolle/ .3 CloudFront

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
aws-foundational-security-best-Praktiken/v/1.0.0/ CloudFront .4	Sicherheitskontrolle/ .4 CloudFront
aws-foundational-security-best-praktiken/v/1.0.0/ CloudFront .5	Sicherheitskontrolle/ .5 CloudFront
aws-foundational-security-best-praktiken/v/1.0.0/ CloudFront .6	Sicherheitskontrolle/ .6 CloudFront
aws-foundational-security-best-praktiken/v/1.0.0/ CloudFront .7	Sicherheitskontrolle/ .7 CloudFront
aws-foundational-security-best-praktiken/v/1.0.0/ CloudFront .8	Sicherheitskontrolle/ .8 CloudFront
aws-foundational-security-best-praktiken/v/1.0.0/ CloudFront .9	Sicherheitskontrolle/ .9 CloudFront
aws-foundational-security-best-praktiken/v/1.0.0/ CloudFront .10	Sicherheitskontrolle/ .10 CloudFront
aws-foundational-security-best-praktiken/v/1.0.0/ CloudFront .12	Sicherheitskontrolle/ .12 CloudFront
aws-foundational-security-best-praktiken/v/1.0.0/ CloudTrail .1	Sicherheitskontrolle/ .1 CloudTrail
aws-foundational-security-best-Praktiken/v/1.0.0/ CloudTrail .2	Sicherheitskontrolle/ .2 CloudTrail
aws-foundational-security-best-praktiken/v/1.0.0/ CloudTrail .4	Sicherheitskontrolle/ .4 CloudTrail
aws-foundational-security-best-praktiken/v/1.0.0/ CloudTrail .5	Sicherheitskontrolle/ .5 CloudTrail

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
aws-foundational-security-best-Praktiken/v/1.0.0/ CodeBuild .1	Sicherheitskontrolle/ .1 CodeBuild
aws-foundational-security-best-Praktiken/v/1.0.0/ CodeBuild .2	Sicherheitskontrolle/ .2 CodeBuild
aws-foundational-security-best-praktiken/v/1.0.0/ CodeBuild .3	Sicherheitskontrolle/ .3 CodeBuild
aws-foundational-security-best-praktiken/v/1.0.0/ CodeBuild .4	Sicherheitskontrolle/ .4 CodeBuild
aws-foundational-security-best-Praktiken/V/1.0.0/Config.1	Sicherheitskontrolle/Config.1
aws-foundational-security-best-Praktiken/V/1.0.0/DMS.1	Sicherheitskontrolle/DMS.1
aws-foundational-security-best-Praktiken / V/1.0.0/DynamoDB.1	Sicherheitskontrolle/DynamoDB.1
aws-foundational-security-best-Praktiken / V/1.0.0/DynamoDB.2	Sicherheitskontrolle/DynamoDB.2
aws-foundational-security-best-Praktiken / V/1.0.0/DynamoDB.3	Sicherheitskontrolle/DynamoDB.3
aws-foundational-security-best-Praktiken / V/1.0.0/EC2.1	Sicherheitskontrolle/EC2.1
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.3	Sicherheitskontrolle/EC2.3
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.4	Sicherheitskontrolle/EC2.4

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.6	Sicherheitskontrolle/EC2.6
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.7	Sicherheitskontrolle/EC2.7
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.8	Sicherheitskontrolle/EC2.8
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.9	Sicherheitskontrolle/EC2.9
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.10	Sicherheitskontrolle/EC2.10
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.15	Sicherheitskontrolle/EC2.15
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.16	Sicherheitskontrolle/EC2.16
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.17	Sicherheitskontrolle/EC2.17
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.18	Sicherheitskontrolle/EC2.18
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.19	Sicherheitskontrolle/EC2.19
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.2	Sicherheitskontrolle/EC2.2
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.20	Sicherheitskontrolle/EC2.20

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.21	Sicherheitskontrolle/EC2.21
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.23	Sicherheitskontrolle/EC2.23
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.24	Sicherheitskontrolle/EC2.24
aws-foundational-security-best-Praktiken/V/1.0.0/EC2.25	Sicherheitskontrolle/EC2.25
aws-foundational-security-best-Praktiken/V/1.0.0/ECR.1	Sicherheitskontrolle/ECR.1
aws-foundational-security-best-Praktiken/V/1.0.0/ECR.2	Sicherheitskontrolle/ECR.2
aws-foundational-security-best-Praktiken/V/1.0.0/ECR.3	Sicherheitskontrolle/ECR.3
aws-foundational-security-best-Praktiken/V/1.0.0/ECS.1	Sicherheitskontrolle/ECS.1
aws-foundational-security-best-Praktiken/V/1.0.0/ECS.10	Sicherheitskontrolle/ECS.10
aws-foundational-security-best-Praktiken/V/1.0.0/ECS.12	Sicherheitskontrolle/ECS.12
aws-foundational-security-best-Praktiken/V/1.0.0/ECS.2	Sicherheitskontrolle/ECS.2
aws-foundational-security-best-Praktiken/V/1.0.0/ECS.3	Sicherheitskontrolle/ECS.3

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
aws-foundational-security-best-Praktiken/V/1.0.0/ECS.4	Sicherheitskontrolle/ECS.4
aws-foundational-security-best-Praktiken/V/1.0.0/ECS.5	Sicherheitskontrolle/ECS.5
aws-foundational-security-best-Praktiken/V/1.0.0/ECS.8	Sicherheitskontrolle/ECS.8
aws-foundational-security-best-Praktiken/V/1.0.0/EFS.1	Sicherheitskontrolle/EFS.1
aws-foundational-security-best-Praktiken/V/1.0.0/EFS.2	Sicherheitskontrolle/EFS.2
aws-foundational-security-best-Praktiken/V/1.0.0/EFS.3	Sicherheitskontrolle/EFS.3
aws-foundational-security-best-Praktiken/V/1.0.0/EFS.4	Sicherheitskontrolle/EFS.4
aws-foundational-security-best-Praktiken/V/1.0.0/EKS.2	Sicherheitskontrolle/EKS.2
aws-foundational-security-best-Praktiken/v/1.0.0/ 1. ElasticBeanstalk	Sicherheitskontrolle/ .1 ElasticBeanstalk
aws-foundational-security-best-Praktiken/v/1.0.0/ ElasticBeanstalk .2	Sicherheitskontrolle/ .2 ElasticBeanstalk
aws-foundational-security-best-Praktiken/V/1.0.0/ELBv2.1	Sicherheitskontrolle/ELB.1
aws-foundational-security-best-Praktiken/V/1.0.0/ELB.2	Sicherheitskontrolle/ELB.2

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
aws-foundational-security-best-Praktiken/V/1.0.0/ELB.3	Sicherheitskontrolle/ELB.3
aws-foundational-security-best-Praktiken/V/1.0.0/ELB.4	Sicherheitskontrolle/ELB.4
aws-foundational-security-best-Praktiken/V/1.0.0/ELB.5	Sicherheitskontrolle/ELB.5
aws-foundational-security-best-Praktiken/V/1.0.0/ELB.6	Sicherheitskontrolle/ELB.6
aws-foundational-security-best-Praktiken/V/1.0.0/ELB.7	Sicherheitskontrolle/ELB.7
aws-foundational-security-best-Praktiken/V/1.0.0/ELB.8	Sicherheitskontrolle/ELB.8
aws-foundational-security-best-Praktiken/V/1.0.0/ELB.9	Sicherheitskontrolle/ELB.9
aws-foundational-security-best-Praktiken/V/1.0.0/ELB.10	Sicherheitskontrolle/ELB.10
aws-foundational-security-best-Praktiken/V/1.0.0/ELB.11	Sicherheitskontrolle/ELB.11
aws-foundational-security-best-Praktiken/V/1.0.0/ELB.12	Sicherheitskontrolle/ELB.12
aws-foundational-security-best-Praktiken/V/1.0.0/ELB.13	Sicherheitskontrolle/ELB.13
aws-foundational-security-best-Praktiken/V/1.0.0/ELB.14	Sicherheitskontrolle/ELB.14

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
aws-foundational-security-best-Praktiken/V/1.0.0/EMR.1	Sicherheitskontrolle/EMR.1
aws-foundational-security-best-Praktiken/V/1.0.0/ES.1	Sicherheitskontrolle/ES.1
aws-foundational-security-best-Praktiken/V/1.0.0/ES.2	Sicherheitskontrolle/ES.2
aws-foundational-security-best-Praktiken/V/1.0.0/ES.3	Sicherheitskontrolle/ES.3
aws-foundational-security-best-Praktiken/V/1.0.0/ES.4	Sicherheitskontrolle/ES.4
aws-foundational-security-best-Praktiken/V/1.0.0/ES.5	Sicherheitskontrolle/ES.5
aws-foundational-security-best-Praktiken/V/1.0.0/ES.6	Sicherheitskontrolle/ES.6
aws-foundational-security-best-Praktiken/V/1.0.0/ES.7	Sicherheitskontrolle/ES.7
aws-foundational-security-best-Praktiken/V/1.0.0/ES.8	Sicherheitskontrolle/ES.8
aws-foundational-security-best-Praktiken/v/1.0.0/ .1 GuardDuty	Sicherheitskontrolle/ .1 GuardDuty
aws-foundational-security-best-Praktiken/V/1.0.0/IAM.1	Sicherheitskontrolle/IAM.1
aws-foundational-security-best-Praktiken/V/1.0.0/IAM.2	Sicherheitskontrolle/IAM.2

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
aws-foundational-security-best-Praktiken/V/1.0.0/IAM.21	Sicherheitskontrolle/IAM.21
aws-foundational-security-best-Praktiken/V/1.0.0/IAM.3	Sicherheitskontrolle/IAM.3
aws-foundational-security-best-Praktiken/V/1.0.0/IAM.4	Sicherheitskontrolle/IAM.4
aws-foundational-security-best-Praktiken/V/1.0.0/IAM.5	Sicherheitskontrolle/IAM.5
aws-foundational-security-best-Praktiken/V/1.0.0/IAM.6	Sicherheitskontrolle/IAM.6
aws-foundational-security-best-Praktiken/V/1.0.0/IAM.7	Sicherheitskontrolle/IAM.7
aws-foundational-security-best-Praktiken/V/1.0.0/IAM.8	Sicherheitskontrolle/IAM.8
aws-foundational-security-best-Praktiken/V/1.0.0/Kinesis.1	Sicherheitskontrolle/Kinesis.1
aws-foundational-security-best-Praktiken / V/1.0.0/KMS.1	Sicherheitskontrolle/KMS.1
aws-foundational-security-best-Praktiken/V/1.0.0/KMS.2	Sicherheitskontrolle/KMS.2
aws-foundational-security-best-Praktiken/V/1.0.0/KMS.3	Sicherheitskontrolle/KMS.3
aws-foundational-security-best-Praktiken/V/1.0.0/Lambda.1	Sicherheitskontrolle/Lambda.1

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
aws-foundational-security-best-Praktiken / V/1.0.0/Lambda.2	Sicherheitskontrolle/Lambda.2
aws-foundational-security-best-Praktiken / V/1.0.0/Lambda.5	Sicherheitskontrolle/Lambda.5
aws-foundational-security-best-praktiken/v/1.0.0/ .3 NetworkFirewall	Sicherheitskontrolle/ .3 NetworkFirewall
aws-foundational-security-best-praktiken/v/1.0.0/ NetworkFirewall .4	Sicherheitskontrolle/ .4 NetworkFirewall
aws-foundational-security-best-praktiken/v/1.0.0/ NetworkFirewall .5	Sicherheitskontrolle/ .5 NetworkFirewall
aws-foundational-security-best-praktiken/v/1.0.0/ NetworkFirewall .6	Sicherheitskontrolle/ .6 NetworkFirewall
aws-foundational-security-best-Praktiken/V/1.0.0/OpenSearch.1	Sicherheitskontrolle/OpenSearch.1
aws-foundational-security-best-Praktiken/V/1.0.0/OpenSearch.2	Sicherheitskontrolle/OpenSearch.2
aws-foundational-security-best-Praktiken/V/1.0.0/OpenSearch.3	Sicherheitskontrolle/OpenSearch.3
aws-foundational-security-best-Praktiken/V/1.0.0/OpenSearch.4	Sicherheitskontrolle/OpenSearch.4
aws-foundational-security-best-Praktiken / V/1.0.0/OpenSearch.5	Sicherheitskontrolle/OpenSearch.5
aws-foundational-security-best-Praktizieren/V/1.0.0/OpenSearch.6	Sicherheitskontrolle/OpenSearch.6

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
aws-foundational-security-best-Praktiken/V/1.0.0/OpenSearch.7	Sicherheitskontrolle/OpenSearch.7
aws-foundational-security-best-Praktizieren/V/1.0.0/OpenSearch.8	Sicherheitskontrolle/OpenSearch.8
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.1	Sicherheitskontrolle/RDS.1
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.10	Sicherheitskontrolle/RDS.10
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.11	Sicherheitskontrolle/RDS.11
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.12	Sicherheitskontrolle/RDS.12
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.13	Sicherheitskontrolle/RDS.13
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.14	Sicherheitskontrolle/RDS.14
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.15	Sicherheitskontrolle/RDS.15
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.16	Sicherheitskontrolle/RDS.16
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.17	Sicherheitskontrolle/RDS.17
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.18	Sicherheitskontrolle/RDS.18

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.19	Sicherheitskontrolle/RDS.19
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.2	Sicherheitskontrolle/RDS.2
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.20	Sicherheitskontrolle/RDS.20
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.21	Sicherheitskontrolle/RDS.21
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.22	Sicherheitskontrolle/RDS.22
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.23	Sicherheitskontrolle/RDS.23
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.24	Sicherheitskontrolle/RDS.24
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.25	Sicherheitskontrolle/RDS.25
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.3	Sicherheitskontrolle/RDS.3
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.4	Sicherheitskontrolle/RDS.4
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.5	Sicherheitskontrolle/RDS.5
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.6	Sicherheitskontrolle/RDS.6

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.7	Sicherheitskontrolle/RDS.7
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.8	Sicherheitskontrolle/RDS.8
aws-foundational-security-best-Praktiken/V/1.0.0/RDS.9	Sicherheitskontrolle/RDS.9
aws-foundational-security-best-Praktiken / V/1.0.0/RedShift.1	Sicherheitskontrolle/RedShift.1
aws-foundational-security-best-Praktiken / V/1.0.0/RedShift.2	Sicherheitssteuerung/RedShift.2
aws-foundational-security-best-Praktiken / V/1.0.0/RedShift.3	Sicherheitskontrolle/RedShift.3
aws-foundational-security-best-Praktiken / V/1.0.0/RedShift.4	Sicherheitssteuerung/RedShift.4
aws-foundational-security-best-Praktiken / V/1.0.0/RedShift.6	Sicherheitssteuerung/RedShift.6
aws-foundational-security-best-Praktiken / V/1.0.0/RedShift.7	Sicherheitssteuerung/RedShift.7
aws-foundational-security-best-Praktiken / V/1.0.0/RedShift.8	Sicherheitssteuerung/RedShift.8
aws-foundational-security-best-Praktiken / V/1.0.0/RedShift.9	Sicherheitssteuerung/RedShift.9
aws-foundational-security-best-Praktiken / V/1.0.0/S3.1	Sicherheitskontrolle/S3.1

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
aws-foundational-security-best-Praktiken/V/1.0.0/S3.12	Sicherheitskontrolle/S3.12
aws-foundational-security-best-Praktiken/V/1.0.0/S3.13	Sicherheitskontrolle/S3.13
aws-foundational-security-best-Praktiken/V/1.0.0/S3.2	Sicherheitskontrolle/S3.2
aws-foundational-security-best-Praktiken/V/1.0.0/S3.3	Sicherheitskontrolle/S3.3
aws-foundational-security-best-Praktiken/V/1.0.0/S3.5	Sicherheitskontrolle/S3.5
aws-foundational-security-best-Praktiken/V/1.0.0/S3.6	Sicherheitskontrolle/S3.6
aws-foundational-security-best-Praktiken/V/1.0.0/S3.8	Sicherheitskontrolle/S3.8
aws-foundational-security-best-Praktiken/V/1.0.0/S3.9	Sicherheitskontrolle/S3.9
aws-foundational-security-best-Praktiken/v/1.0.0/ .1 SageMaker	Sicherheitskontrolle/ .1 SageMaker
aws-foundational-security-best-Praktiken/v/1.0.0/ SageMaker .2	Sicherheitskontrolle/ .2 SageMaker
aws-foundational-security-best-praktiken/v/1.0.0/ SageMaker .3	Sicherheitskontrolle/ .3 SageMaker
aws-foundational-security-best-Praktiken/v/1.0.0/ SecretsManager .1	Sicherheitskontrolle/ .1 SecretsManager

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
aws-foundational-security-best-Praktiken/v/1.0.0/ SecretsManager .2	Sicherheitskontrolle/ .2 SecretsManager
aws-foundational-security-best-praktiken/v/1.0.0/ SecretsManager .3	Sicherheitskontrolle/ .3 SecretsManager
aws-foundational-security-best-praktiken/v/1.0.0/ SecretsManager .4	Sicherheitskontrolle/ .4 SecretsManager
aws-foundational-security-best-Praktiken/V/1.0.0/SQS.1	Sicherheitskontrolle/SQS.1
aws-foundational-security-best-Praktiken/V/1.0.0/SSM.1	Sicherheitskontrolle/SSM.1
aws-foundational-security-best-Praktiken/V/1.0.0/SSM.2	Sicherheitskontrolle/SSM.2
aws-foundational-security-best-Praktiken/V/1.0.0/SSM.3	Sicherheitskontrolle/SSM.3
aws-foundational-security-best-Praktiken/V/1.0.0/SSM.4	Sicherheitskontrolle/SSM.4
aws-foundational-security-best-Praktiken/V/1.0.0/WAF.1	Sicherheitskontrolle/WAF.1
aws-foundational-security-best-Praktiken/V/1.0.0/WAF.2	Sicherheitskontrolle/WAF.2
aws-foundational-security-best-Praktiken/V/1.0.0/WAF.3	Sicherheitskontrolle/WAF.3
aws-foundational-security-best-Praktiken/V/1.0.0/WAF.4	Sicherheitskontrolle/WAF.4

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
aws-foundational-security-best-Praktiken/V/1.0.0/WAF.6	Sicherheitskontrolle/WAF.6
aws-foundational-security-best-Praktiken/V/1.0.0/WAF.7	Sicherheitskontrolle/WAF.7
aws-foundational-security-best-Praktiken/V/1.0.0/WAF.8	Sicherheitskontrolle/WAF.8
aws-foundational-security-best-Praktiken/V/1.0.0/WAF.10	Sicherheitskontrolle/WAF.10
PCI-DSS/V/3.2.1/PCI. AutoScaling1.	Sicherheitskontrolle/ .1 AutoScaling
PCI-DSS/V/3.2.1/PCI. CloudTrail1.	Sicherheitskontrolle/ .2 CloudTrail
PCI-DSS/V/3.2.1/PCI. CloudTrail2.	Sicherheitskontrolle/ .3 CloudTrail
PCI-DSS/V/3.2.1/PCI. CloudTrail3.	Sicherheitskontrolle/ .4 CloudTrail
PCI-DSS/V/3.2.1/PCI. CloudTrail.4	Sicherheitskontrolle/ .5 CloudTrail
PCI-DSS/V/3.2.1/PCI. CodeBuild1.	Sicherheitskontrolle/ .1 CodeBuild
PCI-DSS/V/3.2.1/PCI. CodeBuild2.	Sicherheitskontrolle/ .2 CodeBuild
PCI-DSS/V/3.2.1/PCI.Config.1	Sicherheitskontrolle/Config.1
PCI-DSS/V/3.2.1/PCI.cw.1	Sicherheitskontrolle/ 1. CloudWatch
PCI-DSS/V/3.2.1/PCI.dms.1	Sicherheitskontrolle/DMS.1
PCI-DSS/V/3.2.1/PCI.ec2.1	Sicherheitskontrolle/EC2.1
PCI-DSS/V/3.2.1/PCI.ec2.2	Sicherheitskontrolle/EC2.2
PCI-DSS/V/3.2.1/PCI.ec2.4	Sicherheitskontrolle/EC2.12

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
PCI-DSS/V/3.2.1/PCI.ec2.5	Sicherheitskontrolle/EC2.13
PCI-DSS/V/3.2.1/PCI.ec2.6	Sicherheitskontrolle/EC2.6
PCI-DSS/V/3.2.1/PCI.ELB v2.1	Sicherheitskontrolle/ELB.1
PCI-DSS/V/3.2.1/PCI.ES.1	Sicherheitskontrolle/ES.2
PCI-DSS/V/3.2.1/PCI.es.2	Sicherheitskontrolle/ES.1
PCI-DSS/V/3.2.1/PCI. GuardDuty1.	Sicherheitskontrolle/ .1 GuardDuty
PCI-DSS/V/3.2.1/PCI.IAM.1	Sicherheitskontrolle/IAM.4
PCI-DSS/V/3.2.1/PCI.IAM.2	Sicherheitskontrolle/IAM.2
PCI-DSS/V/3.2.1/PCI.IAM.3	Sicherheitskontrolle/IAM.1
PCI-DSS/V/3.2.1/PCI.IAM.4	Sicherheitskontrolle/IAM.6
PCI-DSS/V/3.2.1/PCI.IAM.5	Sicherheitskontrolle/IAM.9
PCI-DSS/V/3.2.1/PCI.IAM.6	Sicherheitskontrolle/IAM.19
PCI-DSS/V/3.2.1/PCI.IAM.7	Sicherheitskontrolle/IAM.8
PCI-DSS/V/3.2.1/PCI.IAM.8	Sicherheitskontrolle/IAM.10
PCI-DSS/V/3.2.1/PCI.KMS.1	Sicherheitskontrolle/KMS.4
PCI-DSS/V/3.2.1/PCI.Lambda.1	Sicherheitskontrolle/Lambda.1
PCI-DSS/V/3.2.1/PCI.Lambda.2	Sicherheitskontrolle/Lambda.3
PCI-DSS/V/3.2.1/PCI.OpenSearch.1	Sicherheitskontrolle/OpenSearch.2
PCI-DSS/V/3.2.1/PCI.OpenSearch.2	Sicherheitskontrolle/OpenSearch.1
PCI-DSS/V/3.2.1/PCI.RDS.1	Sicherheitskontrolle/RDS.1

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
PCI-DSS/V/3.2.1/PCI.RDS.2	Sicherheitskontrolle/RDS.2
PCI-DSS/V/3.2.1/PCI.RedShift.1	Sicherheitskontrolle/RedShift.1
PCI-DSS/V/3.2.1/PCI.s3.1	Sicherheitskontrolle/S3.3
PCI-DSS/V/3.2.1/PCI.s3.2	Sicherheitskontrolle/S3.2
PCI-DSS/V/3.2.1/PCI.s3.3	Sicherheitskontrolle/S3.7
PCI-DSS/V/3.2.1/PCI.s3.5	Sicherheitskontrolle/S3.5
PCI-DSS/V/3.2.1/PCI.s3.6	Sicherheitskontrolle/S3.1
PCI-DSS/V/3.2.1/PCI. SageMaker1.	Sicherheitskontrolle/ .1 SageMaker
PCI-DSS/V/3.2.1/PCI.SSM.1	Sicherheitskontrolle/SSM.2
PCI-DSS/V/3.2.1/PCI.SSM.2	Sicherheitskontrolle/SSM.3
PCI-DSS/V/3.2.1/PCI.SSM.3	Sicherheitskontrolle/SSM.1
service-managed-aws-control-Turm/V/1.0.0/ACM.1	Sicherheitskontrolle/ACM.1
service-managed-aws-control-Tower/V/1.0.0/APIGateway.1	Sicherheitskontrolle/APIGateway.1
service-managed-aws-control-Tower/V/1.0.0/APIGateway.2	Sicherheitskontrolle/APIGateway.2
service-managed-aws-control-Tower/V/1.0.0/APIGateway.3	Sicherheitskontrolle/APIGateway.3
service-managed-aws-control-Tower/V/1.0.0/APIGateway.4	Sicherheitskontrolle/APIGateway.4

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
service-managed-aws-control-Tower/V/1.0.0/APIGateway.5	Sicherheitskontrolle/APIGateway.5
service-managed-aws-control-turm/v/1.0.0/ .1 AutoScaling	Sicherheitskontrolle/ .1 AutoScaling
service-managed-aws-control-turm/v/1.0.0/ AutoScaling .2	Sicherheitskontrolle/ .2 AutoScaling
service-managed-aws-control-turm/v/1.0.0/ AutoScaling .3	Sicherheitskontrolle/ .3 AutoScaling
service-managed-aws-control-turm/v/1.0.0/ AutoScaling .4	Sicherheitskontrolle/ .4 AutoScaling
service-managed-aws-control-Tower/V/1.0.0/AutoScaling.5	Sicherheitskontrolle/Autoscaling.5
service-managed-aws-control-turm/v/1.0.0/ .6 AutoScaling	Sicherheitskontrolle/ .6 AutoScaling
service-managed-aws-control-turm/v/1.0.0/ AutoScaling .9	Sicherheitskontrolle/ .9 AutoScaling
service-managed-aws-control-turm/v/1.0.0/ CloudTrail .1	Sicherheitskontrolle/ .1 CloudTrail
service-managed-aws-control-turm/v/1.0.0/ CloudTrail .2	Sicherheitskontrolle/ .2 CloudTrail
service-managed-aws-control-turm/v/1.0.0/ CloudTrail .4	Sicherheitskontrolle/ .4 CloudTrail
service-managed-aws-control-turm/v/1.0.0/ CloudTrail .5	Sicherheitskontrolle/ .5 CloudTrail

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
service-managed-aws-control-turm/v/1.0.0/CodeBuild .1	Sicherheitskontrolle/ .1 CodeBuild
service-managed-aws-control-turm/v/1.0.0/CodeBuild .2	Sicherheitskontrolle/ .2 CodeBuild
service-managed-aws-control-turm/v/1.0.0/CodeBuild .4	Sicherheitskontrolle/ .4 CodeBuild
service-managed-aws-control-turm/v/1.0.0/CodeBuild .5	Sicherheitskontrolle/ .5 CodeBuild
service-managed-aws-control-Turm/V/1.0.0/DMS.1	Sicherheitskontrolle/DMS.1
service-managed-aws-control-Turm/V/1.0.0/DynamoDB.1	Sicherheitskontrolle/DynamoDB.1
service-managed-aws-control-Turm/V/1.0.0/DynamoDB.2	Sicherheitskontrolle/DynamoDB.2
service-managed-aws-control-Turm/V/1.0.0/EC2.1	Sicherheitskontrolle/EC2.1
service-managed-aws-control-Turm/V/1.0.0/EC2.2	Sicherheitskontrolle/EC2.2
service-managed-aws-control-Turm/V/1.0.0/EC2.3	Sicherheitskontrolle/EC2.3
service-managed-aws-control-Turm/V/1.0.0/EC2.4	Sicherheitskontrolle/EC2.4
service-managed-aws-control-Turm/V/1.0.0/EC2.6	Sicherheitskontrolle/EC2.6

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
service-managed-aws-control-Turm/V/1.0.0/EC2.7	Sicherheitskontrolle/EC2.7
service-managed-aws-control-Turm/V/1.0.0/EC2.8	Sicherheitskontrolle/EC2.8
service-managed-aws-control-Turm/V/1.0.0/EC2.9	Sicherheitskontrolle/EC2.9
service-managed-aws-control-Turm/V/1.0.0/EC2.10	Sicherheitskontrolle/EC2.10
service-managed-aws-control-Turm/V/1.0.0/EC2.15	Sicherheitskontrolle/EC2.15
service-managed-aws-control-Turm/V/1.0.0/EC2.16	Sicherheitskontrolle/EC2.16
service-managed-aws-control-Turm/V/1.0.0/EC2.17	Sicherheitskontrolle/EC2.17
service-managed-aws-control-Turm/V/1.0.0/EC2.18	Sicherheitskontrolle/EC2.18
service-managed-aws-control-Turm/V/1.0.0/EC2.19	Sicherheitskontrolle/EC2.19
service-managed-aws-control-Turm/V/1.0.0/EC2.20	Sicherheitskontrolle/EC2.20
service-managed-aws-control-Turm/V/1.0.0/EC2.21	Sicherheitskontrolle/EC2.21
service-managed-aws-control-Turm/V/1.0.0/EC2.22	Sicherheitskontrolle/EC2.22

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
service-managed-aws-control-Turm/V/1.0.0/ECR.1	Sicherheitskontrolle/ECR.1
service-managed-aws-control-Turm/V/1.0.0/ECR.2	Sicherheitskontrolle/ECR.2
service-managed-aws-control-Turm/V/1.0.0/ECR.3	Sicherheitskontrolle/ECR.3
service-managed-aws-control-Turm/V/1.0.0/ECS.1	Sicherheitskontrolle/ECS.1
service-managed-aws-control-Turm/V/1.0.0/ECS.2	Sicherheitskontrolle/ECS.2
service-managed-aws-control-Turm/V/1.0.0/ECS.3	Sicherheitskontrolle/ECS.3
service-managed-aws-control-Turm/V/1.0.0/ECS.4	Sicherheitskontrolle/ECS.4
service-managed-aws-control-Turm/V/1.0.0/ECS.5	Sicherheitskontrolle/ECS.5
service-managed-aws-control-Turm/V/1.0.0/ECS.8	Sicherheitskontrolle/ECS.8
service-managed-aws-control-Turm/V/1.0.0/ECS.10	Sicherheitskontrolle/ECS.10
service-managed-aws-control-Turm/V/1.0.0/ECS.12	Sicherheitskontrolle/ECS.12
service-managed-aws-control-Turm/V/1.0.0/EFS.1	Sicherheitskontrolle/EFS.1

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
service-managed-aws-control-Turm/V/1.0.0/EFS.2	Sicherheitskontrolle/EFS.2
service-managed-aws-control-Turm/V/1.0.0/EFS.3	Sicherheitskontrolle/EFS.3
service-managed-aws-control-Turm/V/1.0.0/EFS.4	Sicherheitskontrolle/EFS.4
service-managed-aws-control-Turm/V/1.0.0/EKS.2	Sicherheitskontrolle/EKS.2
service-managed-aws-control-Turm/V/1.0.0/ELB.2	Sicherheitskontrolle/ELB.2
service-managed-aws-control-Turm/V/1.0.0/ELB.3	Sicherheitskontrolle/ELB.3
service-managed-aws-control-Turm/V/1.0.0/ELB.4	Sicherheitskontrolle/ELB.4
service-managed-aws-control-Turm/V/1.0.0/ELB.5	Sicherheitskontrolle/ELB.5
service-managed-aws-control-Turm/V/1.0.0/ELB.6	Sicherheitskontrolle/ELB.6
service-managed-aws-control-Turm/V/1.0.0/ELB.7	Sicherheitskontrolle/ELB.7
service-managed-aws-control-Turm/V/1.0.0/ELB.8	Sicherheitskontrolle/ELB.8
service-managed-aws-control-Turm/V/1.0.0/ELB.9	Sicherheitskontrolle/ELB.9

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
service-managed-aws-control-Turm/V/1.0.0/ELB.10	Sicherheitskontrolle/ELB.10
service-managed-aws-control-Turm/V/1.0.0/ELB.12	Sicherheitskontrolle/ELB.12
service-managed-aws-control-Turm/V/1.0.0/ELB.13	Sicherheitskontrolle/ELB.13
service-managed-aws-control-Turm/V/1.0.0/ELB.14	Sicherheitskontrolle/ELB.14
service-managed-aws-control-Turm/V/1.0.0/ELBv2.1	Sicherheitskontrolle/ELBv2.1
service-managed-aws-control-Turm/V/1.0.0/EMR.1	Sicherheitskontrolle/EMR.1
service-managed-aws-control-Turm/V/1.0.0/ES.1	Sicherheitskontrolle/ES.1
service-managed-aws-control-Turm/V/1.0.0/ES.2	Sicherheitskontrolle/ES.2
service-managed-aws-control-Turm/V/1.0.0/ES.3	Sicherheitskontrolle/ES.3
service-managed-aws-control-Turm/V/1.0.0/ES.4	Sicherheitskontrolle/ES.4
service-managed-aws-control-Turm/V/1.0.0/ES.5	Sicherheitskontrolle/ES.5
service-managed-aws-control-Turm/V/1.0.0/ES.6	Sicherheitskontrolle/ES.6

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
service-managed-aws-control-Turm/V/1.0.0/ES.7	Sicherheitskontrolle/ES.7
service-managed-aws-control-Turm/V/1.0.0/ES.8	Sicherheitskontrolle/ES.8
service-managed-aws-control-turm/v/1.0.0/ .1 ElasticBeanstalk	Sicherheitskontrolle/ .1 ElasticBeanstalk
service-managed-aws-control-turm/v/1.0.0/ElasticBeanstalk .2	Sicherheitskontrolle/ .2 ElasticBeanstalk
service-managed-aws-control-turm/v/1.0.0/GuardDuty .1	Sicherheitskontrolle/ .1 GuardDuty
service-managed-aws-control-Turm/V/1.0.0/IAM.1	Sicherheitskontrolle/IAM.1
service-managed-aws-control-Turm/V/1.0.0/IAM.2	Sicherheitskontrolle/IAM.2
service-managed-aws-control-Turm/V/1.0.0/IAM.3	Sicherheitskontrolle/IAM.3
service-managed-aws-control-Turm/V/1.0.0/IAM.4	Sicherheitskontrolle/IAM.4
service-managed-aws-control-Turm/V/1.0.0/IAM.5	Sicherheitskontrolle/IAM.5
service-managed-aws-control-Turm/V/1.0.0/IAM.6	Sicherheitskontrolle/IAM.6
service-managed-aws-control-Turm/V/1.0.0/IAM.7	Sicherheitskontrolle/IAM.7

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
service-managed-aws-control-Turm/V/1.0.0/IAM.8	Sicherheitskontrolle/IAM.8
service-managed-aws-control-Turm/V/1.0.0/IAM.21	Sicherheitskontrolle/IAM.21
service-managed-aws-control-Turm/V/1.0.0/Kinesis.1	Sicherheitskontrolle/Kinesis.1
service-managed-aws-control-Turm/V/1.0.0/kms.1	Sicherheitskontrolle/KMS.1
service-managed-aws-control-Turm/V/1.0.0/KMS.2	Sicherheitskontrolle/KMS.2
service-managed-aws-control-Turm/V/1.0.0/KMS.3	Sicherheitskontrolle/KMS.3
service-managed-aws-control-Turm/V/1.0.0/Lambda.1	Sicherheitskontrolle/Lambda.1
service-managed-aws-control-Turm/V/1.0.0/Lambda.2	Sicherheitskontrolle/Lambda.2
service-managed-aws-control-Turm/V/1.0.0/Lambda.5	Sicherheitskontrolle/Lambda.5
service-managed-aws-control-turm/v/1.0.0/ 3.NetworkFirewall	Sicherheitskontrolle/ .3 NetworkFirewall
service-managed-aws-control-turm/v/1.0.0/NetworkFirewall .4	Sicherheitskontrolle/ .4 NetworkFirewall
service-managed-aws-control-turm/v/1.0.0/NetworkFirewall .5	Sicherheitskontrolle/ .5 NetworkFirewall

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
service-managed-aws-control-turm/v/1.0.0/NetworkFirewall .6	Sicherheitskontrolle/ .6 NetworkFirewall
service-managed-aws-control-tower/v/1.0.0/OpenSearch.1	Sicherheitskontrolle/OpenSearch.1
service-managed-aws-control-Tower/V/1.0.0/OpenSearch.2	Sicherheitskontrolle/OpenSearch.2
service-managed-aws-control-Tower/V/1.0.0/OpenSearch.3	Sicherheitskontrolle/OpenSearch.3
service-managed-aws-control-Tower/V/1.0.0/OpenSearch.4	Sicherheitskontrolle/OpenSearch.4
service-managed-aws-control-Tower/V/1.0.0/OpenSearch.5	Sicherheitskontrolle/OpenSearch.5
service-managed-aws-control-Tower/V/1.0.0/OpenSearch.6	Sicherheitskontrolle/OpenSearch.6
service-managed-aws-control-Tower/V/1.0.0/OpenSearch.7	Sicherheitskontrolle/OpenSearch.7
service-managed-aws-control-Tower/V/1.0.0/OpenSearch.8	Sicherheitskontrolle/OpenSearch.8
service-managed-aws-control-Turm/V/1.0.0/RDS.1	Sicherheitskontrolle/RDS.1
service-managed-aws-control-Turm/V/1.0.0/RDS.2	Sicherheitskontrolle/RDS.2
service-managed-aws-control-Turm/V/1.0.0/RDS.3	Sicherheitskontrolle/RDS.3

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
service-managed-aws-control-Turm/V/1.0.0/RDS.4	Sicherheitskontrolle/RDS.4
service-managed-aws-control-Turm/V/1.0.0/RDS.5	Sicherheitskontrolle/RDS.5
service-managed-aws-control-Turm/V/1.0.0/RDS.6	Sicherheitskontrolle/RDS.6
service-managed-aws-control-Turm/V/1.0.0/RDS.8	Sicherheitskontrolle/RDS.8
service-managed-aws-control-Turm/V/1.0.0/RDS.9	Sicherheitskontrolle/RDS.9
service-managed-aws-control-Turm/V/1.0.0/RDS.10	Sicherheitskontrolle/RDS.10
service-managed-aws-control-Turm/V/1.0.0/RDS.11	Sicherheitskontrolle/RDS.11
service-managed-aws-control-Turm/V/1.0.0/RDS.13	Sicherheitskontrolle/RDS.13
service-managed-aws-control-Turm/V/1.0.0/RDS.17	Sicherheitskontrolle/RDS.17
service-managed-aws-control-Turm/V/1.0.0/RDS.18	Sicherheitskontrolle/RDS.18
service-managed-aws-control-Turm/V/1.0.0/RDS.19	Sicherheitskontrolle/RDS.19
service-managed-aws-control-Turm/V/1.0.0/RDS.20	Sicherheitskontrolle/RDS.20

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
service-managed-aws-control-Turm/V/1.0.0/RDS.21	Sicherheitskontrolle/RDS.21
service-managed-aws-control-Turm/V/1.0.0/RDS.22	Sicherheitskontrolle/RDS.22
service-managed-aws-control-Turm/V/1.0.0/RDS.23	Sicherheitskontrolle/RDS.23
service-managed-aws-control-Turm/V/1.0.0/RDS.25	Sicherheitskontrolle/RDS.25
service-managed-aws-control-Turm/V/1.0.0/RedShift.1	Sicherheitskontrolle/RedShift.1
service-managed-aws-control-Turm/V/1.0.0/RedShift.2	Sicherheitssteuerung/RedShift.2
service-managed-aws-control-Turm/V/1.0.0/RedShift.4	Sicherheitssteuerung/RedShift.4
service-managed-aws-control-Turm/V/1.0.0/RedShift.6	Sicherheitssteuerung/RedShift.6
service-managed-aws-control-Turm/V/1.0.0/RedShift.7	Sicherheitssteuerung/RedShift.7
service-managed-aws-control-Turm/V/1.0.0/RedShift.8	Sicherheitssteuerung/RedShift.8
service-managed-aws-control-Turm/V/1.0.0/RedShift.9	Sicherheitssteuerung/RedShift.9
service-managed-aws-control-Turm/V/1.0.0/S3.1	Sicherheitskontrolle/S3.1

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
service-managed-aws-control-Turm/V/1.0.0/S3.2	Sicherheitskontrolle/S3.2
service-managed-aws-control-Turm/V/1.0.0/S3.3	Sicherheitskontrolle/S3.3
service-managed-aws-control-Turm/V/1.0.0/S3.5	Sicherheitskontrolle/S3.5
service-managed-aws-control-Turm/V/1.0.0/S3.6	Sicherheitskontrolle/S3.6
service-managed-aws-control-Turm/V/1.0.0/S3.8	Sicherheitskontrolle/S3.8
service-managed-aws-control-Turm/V/1.0.0/S3.9	Sicherheitskontrolle/S3.9
service-managed-aws-control-Turm/V/1.0.0/S3.12	Sicherheitskontrolle/S3.12
service-managed-aws-control-Turm/V/1.0.0/S3.13	Sicherheitskontrolle/S3.13
service-managed-aws-control-turm/v/1.0.0/ .1 SageMaker	Sicherheitskontrolle/ .1 SageMaker
service-managed-aws-control-turm/v/1.0.0/SecretsManager .1	Sicherheitskontrolle/ .1 SecretsManager
service-managed-aws-control-turm/v/1.0.0/SecretsManager .2	Sicherheitskontrolle/ .2 SecretsManager
service-managed-aws-control-turm/v/1.0.0/SecretsManager .3	Sicherheitskontrolle/ .3 SecretsManager

GeneratorID vor der Aktivierung der konsolidierten Kontrollergebnisse	GeneratorID nach dem Einschalten der konsolidierten Kontrollergebnisse
service-managed-aws-control-turm/v/1.0.0/SecretsManager .4	Sicherheitskontrolle/ .4 SecretsManager
service-managed-aws-control-Turm/V/1.0.0/SQS.1	Sicherheitskontrolle/SQS.1
service-managed-aws-control-Turm/V/1.0.0/SSM.1	Sicherheitskontrolle/SSM.1
service-managed-aws-control-Turm/V/1.0.0/SSM.2	Sicherheitskontrolle/SSM.2
service-managed-aws-control-Turm/V/1.0.0/SSM.3	Sicherheitskontrolle/SSM.3
service-managed-aws-control-Turm/V/1.0.0/SSM.4	Sicherheitskontrolle/SSM.4
service-managed-aws-control-Turm/V/1.0.0/WAF.2	Sicherheitskontrolle/WAF.2
service-managed-aws-control-Turm/V/1.0.0/WAF.3	Sicherheitskontrolle/WAF.3
service-managed-aws-control-Turm/V/1.0.0/WAF.4	Sicherheitskontrolle/WAF.4

Wie sich die Konsolidierung auf Kontroll-IDs und Titel auswirkt

Die Ansicht konsolidierter Kontrollen und die konsolidierten Kontrollergebnisse vereinheitlichen die Kontroll-IDs und Titel für alle Standards. Die Begriffe Security Control ID und Security Control Title beziehen sich auf diese standardunabhängigen Werte. Die folgende Tabelle zeigt die Zuordnung von IDs und Titeln für Sicherheitskontrollen zu standardspezifischen Kontroll-IDs und Titeln. IDs und Titel für Steuerelemente, die zum FSBP-Standard (AWS Foundation Security Best Practices) gehören, bleiben unverändert.

In der Security Hub Hub-Konsole werden Sicherheitskontroll-IDs und Sicherheitskontrolltitel angezeigt, unabhängig davon, ob die konsolidierten Kontrollergebnisse in Ihrem Konto aktiviert oder deaktiviert sind. Security Hub Hub-Ergebnisse enthalten Sicherheitskontroll-IDs und Sicherheitskontrolltitel jedoch nur, wenn konsolidierte Kontrollergebnisse in Ihrem Konto aktiviert sind. Wenn konsolidierte Kontrollergebnisse in Ihrem Konto deaktiviert sind, enthalten die Security Hub Hub-Ergebnisse standardspezifische Kontroll-IDs und Titel. Weitere Informationen darüber, wie sich die Konsolidierung auf die Kontrollergebnisse auswirkt, finden Sie unter. Ergebnisse der Stichprobenkontrolle

Bei Kontrollen, die Teil von Service-Managed Standard: sind AWS Control Tower, `CT.` wird das Präfix aus der Kontroll-ID und dem Titel in den Ergebnissen entfernt, wenn konsolidierte Kontrollergebnisse aktiviert werden.

Um Ihre eigenen Skripts für diese Tabelle auszuführen, laden Sie sie als CSV-Datei herunter.

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	1.1 Vermeiden Sie die Verwendung des Root-Benutzers	[CloudWatch.1] Für den Benutzer „root“ sollten ein Metrik-Logfilter und ein Alarm vorhanden sein
CIS v1.2.0	1.10 Stellen Sie sicher, dass die IAM-Kennwortrichtlinie die Wiederverwendung von Passwörtern	[IAM.16] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert
CIS v1.2.0	1.11 Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft	[IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft
CIS v1.2.0	1.12 Stellen Sie sicher, dass kein Root-Benutzerzugriffsschlüssel vorhanden ist	[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
CIS v1.2.0	1.13 Stellen Sie sicher, dass MFA für den Root-Benutzer aktiviert ist	[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	1.14 Stellen Sie sicher, dass Hardware-MFA für den Root-Benutzer aktiviert ist	[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.
CIS v1.2.0	1.16 Stellen Sie sicher, dass IAM-Richtlinien nur Gruppen oder Rollen zugeordnet sind	[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
CIS v1.2.0	1.2 Stellen Sie sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen	[IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen
CIS v1.2.0	1.20 Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support	[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
CIS v1.2.0	1.22 Stellen Sie sicher, dass keine IAM-Richtlinien erstellt werden, die volle „*: *“ -Administratorrechte zulassen	[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
CIS v1.2.0	1.3 Stellen Sie sicher, dass Anmeldeinformationen, die 90 Tage oder länger nicht verwendet wurden, deaktiviert sind	[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
CIS v1.2.0	1.4 Stellen Sie sicher, dass die Zugangsschlüssel alle 90 Tage oder weniger gewechselt werden	[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
CIS v1.2.0	1.5 Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert	[IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	1.6 Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert	[IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert
CIS v1.2.0	1.7 Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist	[IAM.13] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist
CIS v1.2.0	1.8 Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert	[IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert
CIS v1.2.0	1.9 Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert	[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
CIS v1.2.0	2.1 Stellen Sie sicher, dass CloudTrail es in allen Regionen aktiviert ist	[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst
CIS v1.2.0	2.2 Stellen CloudTrail Sie sicher, dass die Überprüfung der Protokolldatei aktiviert ist	[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein
CIS v1.2.0	2.3 Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist	[CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist
CIS v1.2.0	2.4 Stellen Sie sicher, dass die CloudTrail Pfade in CloudWatch Logs integriert sind	[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	2.5 Stellen Sie sicher, dass AWS Config es aktiviert ist	[Config.1] AWS Config sollte aktiviert sein
CIS v1.2.0	2.6 Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist	[CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket -Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist
CIS v1.2.0	2.7 Stellen Sie sicher, dass die CloudTrail Protokolle im Ruhezusta nd mithilfe von KMS-CMKs verschlüs selt werden	[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben
CIS v1.2.0	2.8 Stellen Sie sicher, dass die Rotation für vom Kunden erstellte CMKs aktiviert ist	[KMS.4] Die AWS KMS Schlüssel rotation sollte aktiviert sein
CIS v1.2.0	2.9 Stellen Sie sicher, dass die VPC-Flussprotokollierung in allen VPCs aktiviert ist	[EC2.6] Die VPC-Flow-Protokoll ierung sollte in allen VPCs aktiviert sein
CIS v1.2.0	3.1 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind	[CloudWatch.2] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für nicht autorisierte API-Aufru fe vorhanden sind
CIS v1.2.0	3.10 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind	[CloudWatch.10] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherhei tsgruppen vorhanden sind
CIS v1.2.0	3.11 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind	[CloudWatch.11] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	3.12 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind	[CloudWatch.12] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind
CIS v1.2.0	3.13 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind	[CloudWatch.13] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind
CIS v1.2.0	3.14 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind	[CloudWatch.14] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind
CIS v1.2.0	3.2 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Anmeldung in der Management Console ohne MFA vorhanden sind	[CloudWatch.3] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Anmeldung an der Management Console ohne MFA vorhanden sind
CIS v1.2.0	3.3 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Verwendung des Root-Benutzers vorhanden sind	[CloudWatch.1] Für den Benutzer „root“ sollten ein Metrik-Logfilter und ein Alarm vorhanden sein
CIS v1.2.0	3.4 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der IAM-Richtlinien vorhanden sind	[CloudWatch.4] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für IAM-Richtlinienänderungen vorhanden sind
CIS v1.2.0	3.5 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind	[CloudWatch1.5] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der Dauer CloudTrail AWS Config vorhanden sind

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.2.0	3.6 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Management Console Authentif izierungsfehler vorhanden sind	[CloudWatch.6] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind
CIS v1.2.0	3.7 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden erstellten CMKs vorhanden sind	[CloudWatch.7] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind
CIS v1.2.0	3.8 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der S3-Bucket-Richtlinie vorhanden sind	[CloudWatch.8] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind
CIS v1.2.0	3.9 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Config Konfigurationsänderungen vorhanden sind	[CloudWatch.9] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Config Konfigura tionsänderungen vorhanden sind
CIS v1.2.0	4.1 Stellen Sie sicher, dass keine Sicherheitsgruppen den Zugang von 0.0.0.0/0 zu Port 22 zulassen	[EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen
CIS v1.2.0	4.2 Stellen Sie sicher, dass keine Sicherheitsgruppen den Zugriff von 0.0.0.0/0 auf Port 3389 zulassen	[EC2.14] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulassen
CIS v1.2.0	4.3 Stellen Sie sicher, dass die Standardsicherheitsgruppe jeder VPC den gesamten Datenverkehr einschränkt	[EC2.2] VPC-Standardsicher heitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.4.0	1.10 Stellen Sie sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist, die über ein Konsolenpasswort verfügen	[IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen
CIS v1.4.0	1.14 Stellen Sie sicher, dass die Zugangsschlüssel alle 90 Tage oder weniger gewechselt werden	[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
CIS v1.4.0	1.16 Stellen Sie sicher, dass IAM-Richtlinien, die volle „*: *“ -Administratorrechte zulassen, nicht beigefügt sind	[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
CIS v1.4.0	1.17 Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support	[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
CIS v1.4.0	1.4 Stellen Sie sicher, dass kein Zugriffsschlüssel für das Root-Benutzerkonto vorhanden ist	[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
CIS v1.4.0	1.5 Stellen Sie sicher, dass MFA für das Root-Benutzerkonto aktiviert ist	[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
CIS v1.4.0	1.6 Stellen Sie sicher, dass Hardware-MFA für das Root-Benutzerkonto aktiviert ist	[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.
CIS v1.4.0	1.7 Eliminieren Sie die Verwendung des Root-Benutzers für administrative und tägliche Aufgaben	[CloudWatch.1] Für den Benutzer „root“ sollten ein Metrik-Logfilter und ein Alarm vorhanden sein

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.4.0	1.8 Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestlänge von 14 oder mehr erfordert	[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
CIS v1.4.0	1.9 Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederver wendung von	[IAM.16] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederver wendung von Passwörtern verhindert
CIS v1.4.0	2.1.2 Stellen Sie sicher, dass die S3-Bucket-Richtlinie so eingestellt ist, dass HTTP-Anfragen abgelehnt werden	[S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern
CIS v1.4.0	2.1.5.1 Die Einstellung S3 Block Public Access sollte aktiviert sein	[S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein
CIS v1.4.0	2.1.5.2 Die Einstellung S3 Block Public Access sollte auf Bucket-Eb ene aktiviert sein	[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren
CIS v1.4.0	2.2.1 Stellen Sie sicher, dass die EBS-Volume-Verschlüsselung aktiviert ist	[EC2.7] Die EBS-Standardversch lüsselung sollte aktiviert sein
CIS v1.4.0	2.3.1 Stellen Sie sicher, dass die Verschlüsselung für RDS-Instances aktiviert ist	[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.4.0	3.1 Stellen Sie sicher, dass CloudTrail es in allen Regionen aktiviert ist	[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst
CIS v1.4.0	3.2 Stellen CloudTrail Sie sicher, dass die Überprüfung der Protokolldatei aktiviert ist	[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein
CIS v1.4.0	3.4 Stellen Sie sicher, dass die CloudTrail Pfade in Logs integriert CloudWatch sind	[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden
CIS v1.4.0	3.5 Stellen Sie sicher, dass AWS Config es in allen Regionen aktiviert ist	[Config.1] AWS Config sollte aktiviert sein
CIS v1.4.0	3.6 Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist	[CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist
CIS v1.4.0	3.7 Stellen Sie sicher, dass die CloudTrail Protokolle im Ruhezustand mithilfe von KMS-CMKs verschlüsselt werden	[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben
CIS v1.4.0	3.8 Stellen Sie sicher, dass die Rotation für vom Kunden erstellte CMKs aktiviert ist	[KMS.4] Die AWS KMS Schlüsselrotation sollte aktiviert sein
CIS v1.4.0	3.9 Stellen Sie sicher, dass die VPC-Flussprotokollierung in allen VPCs aktiviert ist	[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.4.0	4.4 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der IAM-Richtlinien vorhanden sind	[CloudWatch.4] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für IAM-Richtlinienänderungen vorhanden sind
CIS v1.4.0	4.5 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind	[CloudWatch1.5] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der Dauer CloudTrail AWS Config vorhanden sind
CIS v1.4.0	4.6 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Management Console Authentif izierungsfehler vorhanden sind	[CloudWatch.6] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind
CIS v1.4.0	4.7 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden erstellten CMKs vorhanden sind	[CloudWatch.7] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind
CIS v1.4.0	4.8 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind	[CloudWatch.8] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind
CIS v1.4.0	4.9 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Config Konfigurationsänderungen vorhanden sind	[CloudWatch.9] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Config Konfigura tionsänderungen vorhanden sind

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
CIS v1.4.0	4.10 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind	[CloudWatch.10] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind
CIS v1.4.0	4.11 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind	[CloudWatch.11] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind
CIS v1.4.0	4.12 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind	[CloudWatch.12] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind
CIS v1.4.0	4.13 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind	[CloudWatch.13] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind
CIS v1.4.0	4.14 Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind	[CloudWatch.14] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind
CIS v1.4.0	5.1 Stellen Sie sicher, dass keine Netzwerk-ACLs den Zugriff von 0.0.0.0/0 zu den Verwaltungsports des Remoteservers zulassen	[EC2.21] Netzwerk-ACLs sollten keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen
CIS v1.4.0	5.3 Stellen Sie sicher, dass die Standardsicherheitsgruppe jeder VPC den gesamten Datenverkehr einschränkt	[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
PCI DSS v3.2.1	PCI. AutoScaling.1 Auto Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten Load Balancer-Integritätsprüfungen verwenden	[AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden
PCI DSS v3.2.1	PCI. CloudTrail.1 CloudTrail Protokolle sollten im Ruhezustand mit AWS KMS CMKs verschlüsselt werden	[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben
PCI DSS v3.2.1	PCI. CloudTrail.2 CloudTrail sollte aktiviert sein	[CloudTrail.3] Mindestens ein CloudTrail Trail sollte aktiviert sein
PCI DSS v3.2.1	PCI. CloudTrail.3 Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein	[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein
PCI DSS v3.2.1	PCI. CloudTrail.4 CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden	[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden
PCI DSS v3.2.1	PCI. CodeBuild.1 CodeBuild GitHub - oder Bitbucket-Quell-Repository-URLs sollten OAuth verwenden	[CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
PCI DSS v3.2.1	PCI. CodeBuild.2 CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten	[CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
PCI DSS v3.2.1	AWS Config PCI.Config.1 sollte aktiviert sein	[Config.1] AWS Config sollte aktiviert sein

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
PCI DSS v3.2.1	PCI.CW.1 Es sollten ein Log-Metrikfilter und ein Alarm für die Verwendung durch den Benutzer „root“ vorhanden sein	[CloudWatch.1] Für den Benutzer „root“ sollten ein Metrik-Logfilter und ein Alarm vorhanden sein
PCI DSS v3.2.1	PCI.DMS.1 Database Migration Service Service-Replikationsinstanzen sollten nicht öffentlich sein	[DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
PCI DSS v3.2.1	PCI.EC2.1 EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein	[EC2.1] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein
PCI DSS v3.2.1	Die VPC-Standardsicherheitsgruppe PCI.EC2.2 sollte eingehenden und ausgehenden Datenverkehr verbieten	[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen
PCI DSS v3.2.1	PCI.EC2.4 Ungenutzte EC2-EIPs sollten entfernt werden	[EC2.12] Ungenutzte Amazon EC2 EC2-EIPs sollten entfernt werden
PCI DSS v3.2.1	PCI.EC2.5-Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 auf Port 22 zulassen	[EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen
PCI DSS v3.2.1	PCI.EC2.6 Die VPC-Flussprotokollierung sollte in allen VPCs aktiviert sein	[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein
PCI DSS v3.2.1	PCI.ELBv2.1 Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden	[ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden
PCI DSS v3.2.1	PCI.ES.1 Elasticsearch-Domains sollten sich in einer VPC befinden	[ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
PCI DSS v3.2.1	Bei PCI.ES.2 Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein	[ES.1] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
PCI DSS v3.2.1	PCI. GuardDuty.1 GuardDuty sollte aktiviert sein	[GuardDuty.1] GuardDuty sollte aktiviert sein
PCI DSS v3.2.1	PCI.IAM.1 Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren	[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
PCI DSS v3.2.1	PCI.IAM.2 IAM-Benutzern sollten keine IAM-Richtlinien zugewiesen sein	[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
PCI DSS v3.2.1	PCI.IAM.3 IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen	[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
PCI DSS v3.2.1	PCI.IAM.4 Hardware MFA sollte für den Root-Benutzer aktiviert sein	[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.
PCI DSS v3.2.1	PCI.IAM.5 Virtual MFA sollte für den Root-Benutzer aktiviert sein	[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
PCI DSS v3.2.1	PCI.IAM.6 MFA sollte für alle IAM-Benutzer aktiviert sein	[IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
PCI DSS v3.2.1	PCI.IAM.7 IAM-Benutzeranmeldedaten sollten deaktiviert werden, wenn sie nicht innerhalb einer vordefinierten Anzahl von Tagen verwendet werden	[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
PCI DSS v3.2.1	PCI.IAM.8-Passwortrichtlinien für IAM-Benutzer sollten solide Konfigurationen haben	[IAM.10] Passwortrichtlinien für IAM-Benutzer sollten strenge Laufzeiten haben AWS Config

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
PCI DSS v3.2.1	PCI.KMS.1 Die CMK-Rotation (Customer Master Key) sollte aktiviert sein	[KMS.4] Die AWS KMS Schlüssel rotation sollte aktiviert sein
PCI DSS v3.2.1	PCI.Lambda.1 Lambda-Funktionen sollten den öffentlichen Zugriff verbieten	[Lambda.1] Lambda-Funktionsri chtlinien sollten den öffentlichen Zugriff verbieten
PCI DSS v3.2.1	PCI.Lambda.2 Lambda-Funktionen sollten sich in einer VPC befinden	[Lambda.3] Lambda-Funktionen sollten sich in einer VPC befinden
PCI DSS v3.2.1	OpenSearch PCI.OpenSearch.1-Domains sollten sich in einer VPC befinden	[Opensearch.2] OpenSearch - Domains sollten nicht öffentlich zugänglich sein
PCI DSS v3.2.1	PCI.OpenSearch.2 EBS-Snapshots sollten nicht öffentlich wiederher stellbar sein	Bei [Opensearch.1] OpenSearch - Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
PCI DSS v3.2.1	Der PCI.RDS.1 RDS-Snapshot sollte privat sein	[RDS.1] Der RDS-Snapshot sollte privat sein
PCI DSS v3.2.1	PCI.RDS.2 RDS-DB-Instances sollten den öffentlichen Zugriff verbieten	[RDS.2] RDS-DB-Instances sollten je nach Dauer den öffentlichen Zugriff verbieten PubliclyAccessible AWS Config
PCI DSS v3.2.1	PCI.redshift.1 Amazon Redshift Redshift-Cluster sollten den öffentlic hen Zugriff verbieten	[Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlic hen Zugriff verbieten
PCI DSS v3.2.1	PCI.S3.1 S3-Buckets sollten öffentlic hen Schreibzugriff verbieten	[S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
PCI DSS v3.2.1	PCI.S3.2 S3-Buckets sollten öffentlichen Lesezugriff verbieten	[S3.2] S3-Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren
PCI DSS v3.2.1	Bei PCI.S3.3 S3-Buckets sollte die regionsübergreifende Replikation aktiviert sein	[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden
PCI DSS v3.2.1	PCI.S3.5 S3-Buckets sollten Anfragen zur Verwendung von Secure Socket Layer erfordern	[S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern
PCI DSS v3.2.1	Die Einstellung PCI.S3.6 S3 Block Public Access sollte aktiviert sein	[S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein
PCI DSS v3.2.1	PCI. SageMaker.1 SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben	[SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
PCI DSS v3.2.1	PCI.SSM.1 EC2-Instances, die von Systems Manager verwaltet werden, sollten nach einer Patch-Installation den Patch-Konformitätsstatus COMPLIANT haben	[SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
PCI DSS v3.2.1	Von Systems Manager verwaltete PCI.SSM.2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben	[SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben

Standard	Standard-Kontroll-ID und Titel	ID und Titel der Sicherheitskontrolle
PCI DSS v3.2.1	PCI.SSM.3 EC2-Instances sollten verwaltet werden von AWS Systems Manager	[SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager

Aktualisierung der Workflows für die Konsolidierung

Wenn Ihre Workflows nicht auf dem spezifischen Format der Kontrollergebnisfelder basieren, sind keine Maßnahmen erforderlich.

Wenn Ihre Workflows auf dem spezifischen Format der in den Tabellen angegebenen Kontrollfindungsfelder basieren, sollten Sie Ihre Workflows aktualisieren. Wenn Sie beispielsweise eine Amazon CloudWatch Events-Regel erstellt haben, die eine Aktion für eine bestimmte Kontroll-ID ausgelöst hat (z. B. das Aufrufen einer AWS Lambda Funktion, wenn die Kontroll-ID CIS 2.7 entspricht), aktualisieren Sie die Regel so, dass sie CloudTrail .2, das `Compliance.SecurityControlId` Feld für dieses Steuerelement, verwendet.

Wenn Sie benutzerdefinierte Erkenntnisse mithilfe von Feldern oder Werten für die Kontrollsuche erstellt haben, die sich geändert haben, aktualisieren Sie diese Erkenntnisse, sodass sie die aktuellen Felder oder Werte verwenden.

ASFF-Beispiele

Die folgenden Abschnitte enthalten Beispiele für erforderliche und optionale Attribute im AWS Security Finding Format (ASFF) sowie Beispiele für jede Ressource, die ASFF unterstützt.

Themen

- Erforderliche Attribute der obersten Ebene
- Optionale Attribute der obersten Ebene
- Resources

Erforderliche Attribute der obersten Ebene

Die folgenden Attribute der obersten Ebene im AWS Security Finding Format (ASFF) sind für alle Ergebnisse in Security Hub erforderlich. Weitere Informationen zu diesen erforderlichen Attributen finden Sie AwsSecurityFindingin der AWS Security Hub API-Referenz.

AwsAccountId

Die AWS-Konto ID, für die der Befund gilt.

Beispiel

```
"AwsAccountId": "111111111111"
```

CreatedAt

Gibt an, wann das potenzielle Sicherheitsproblem, das durch einen Befund erkannt wurde, verursacht wurde.

Beispiel

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

> **Note**
>
> Security Hub löscht Ergebnisse 90 Tage nach dem letzten Update oder 90 Tage nach dem Erstellungsdatum, wenn kein Update erfolgt. Um Ergebnisse länger als 90 Tage zu speichern, können Sie in Amazon eine Regel konfigurieren EventBridge , die Ergebnisse an Ihren S3-Bucket weiterleitet.

Beschreibung

Die Beschreibung eines Fundes. Dieses Feld kann unspezifischen Standardtext oder spezifische Details für die Instance des Fundes enthalten.

Für Kontrollergebnisse, die Security Hub generiert, enthält dieses Feld eine Beschreibung der Kontrolle.

Dieses Feld verweist nicht auf einen Standard, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

Beispiel

```
"Description": "This AWS control checks whether AWS Config is enabled in the current
 account and Region."
```

GeneratorId

Die Kennung für die lösungsspezifische Komponente (eine separate Logikeinheit), die einen Fund generiert hat.

Bei Kontrollergebnissen, die Security Hub generiert, verweist dieses Feld nicht auf einen Standard, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

Beispiel

```
"GeneratorId": "security-control/Config.1"
```

Id

Die produktspezifische Kennung für einen Fund. Für Kontrollergebnisse, die Security Hub generiert, enthält dieses Feld den Amazon-Ressourcennamen (ARN) des Ergebnisses.

Dieses Feld verweist nicht auf einen Standard, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

Beispiel

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/
ab6d6a26-a156-48f0-9403-115983e5a956

"
```

ProductArn

Der von Security Hub generierte Amazon-Ressourcenname (ARN), der ein Produkt eines Drittanbieters eindeutig identifiziert, nachdem das Produkt bei Security Hub registriert wurde.

Das Format des Felds ist `arn:`*`partition`*`:securityhub:`*`region`*`:`*`account-id`*`:product/`*`company-id`*`/`*`product-id`*.

- Für AWS Dienste, die in Security Hub integriert sind, `company-id` muss das "`aws`" lauten, und das `product-id` muss der AWS öffentliche Dienstname sein. Da AWS Produkte und Dienstleistungen keinem Konto zugeordnet sind, ist der `account-id` Bereich des ARN leer. AWS Dienste, die noch nicht in Security Hub integriert sind, gelten als Produkte von Drittanbietern.
- Für öffentliche Produkte müssen die `company-id` und die `product-id` die ID-Werte sein, die zum Zeitpunkt der Registrierung angegeben wurden.

- Für private Produkte muss die `company-id` die Konto-ID sein. Die `product-id` muss das reservierte Wort "default" (Standard) oder die ID sein, die zum Zeitpunkt der Registrierung angegeben wurde.

Beispiel

```
// Private ARN
    "ProductArn": "arn:aws:securityhub:us-east-1:111111111111:product/111111111111/
default"

// Public ARN

    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty"
    "ProductArn": "arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-
pro"
```

Ressourcen

Das `Resources`Objekt stellt eine Reihe von Ressourcendatentypen bereit, die die AWS Ressourcen beschreiben, auf die sich das Ergebnis bezieht.

Beispiel

```
"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0",
    "ApplicationName": "SampleApp",
    "DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
```

```
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
                        "Occurrences": {
                            "Pages": [
                                {
                                    "PageNumber": 1,
                                    "OffsetRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                     },
                                    "LineRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                    }
                                }
                            ]
                        }
                    },
                    {
                        "Count": 2229,
                        "Type": "URL",
                        "Occurrences": {
                           "LineRanges": [
                               {
                                   "Start": 1,
```

```
                                "End": 13
                            }
                        ]
                    }
                },
                {
                    "Count": 13826,
                    "Type": "NameDetection",
                    "Occurrences": {
                         "Records": [
                             {
                                 "RecordIndex": 1,
                                 "JsonPath": "$.ssn.value"
                             }
                         ]
                     }
                },
                {
                    "Count": 32,
                    "Type": "AddressDetection"
                }
            ],
            "TotalCount": 32
        }
    ],
    "CustomDataIdentifiers": {
        "Detections": [
            {
                "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                "Name": "1712be25e7c7f53c731fe464f1c869b8",
                "Count": 2,
            }
        ],
        "TotalCount": 2
    }
  }
},
 "Type": "AwsEc2Instance",
 "Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
 "Partition": "aws",
 "Region": "us-west-2",
 "ResourceRole": "Target",
 "Tags": {
  "billingCode": "Lotus-1-2-3",
```

```
  "needsPatching": true
 },
 "Details": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
  "ImageId": "ami-79fd7eee",
  "IpV4Addresses": ["1.1.1.1"],
  "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
  "KeyName": "testkey",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "MetadataOptions": {
   "HttpEndpoint": "enabled",
   "HttpProtocolIpv6": "enabled",
   "HttpPutResponseHopLimit": 1,
   "HttpTokens": "optional",
   "InstanceMetadataTags": "disabled"
  }
 },
  "NetworkInterfaces": [
  {
   "NetworkInterfaceId": "eni-e5aa89a3"
  }
  ],
  "SubnetId": "PublicSubnet",
  "Type": "i3.xlarge",
  "VirtualizationType": "hvm",
  "VpcId": "TestVPCIpv6"
 }

]
```

SchemaVersion

Die Schemaversion, für die ein Fund formatiert ist. Der Wert dieses Feldes muss eine der offiziell veröffentlichten Versionen sein, die von AWS identifiziert wurden. In der aktuellen Version lautet die Schemaversion des AWS Security Finding Formats`2018-10-08`.

Beispiel

```
"SchemaVersion": "2018-10-08"
```

Schweregrad

Definiert die Wichtigkeit eines Ergebnisses. Einzelheiten zu diesem Objekt finden Sie `Severity`in der AWS Security Hub API-Referenz.

`Severity`ist sowohl ein Objekt der obersten Ebene in einem Finding als auch ein unter dem Objekt verschachteltes Objekt. `FindingProviderFields`

Der Wert des `Severity` Objekts der obersten Ebene für einen Befund sollte nur von der API aktualisiert werden. `BatchUpdateFindings`

Um Informationen zum Schweregrad bereitzustellen, sollten Finding-Provider das `Severity` Objekt unter aktualisieren`FindingProviderFields`, wenn eine `BatchImportFindings`API-Anfrage gestellt wird.
Wenn eine `BatchImportFindings` Anfrage für ein neues Ergebnis nur liefert `Label` oder nur liefert`Normalized`, füllt Security Hub automatisch den Wert des anderen Felds aus. Das `Product` Feld unter `FindingProviderFields` ist deaktiviert und wird in den aktuellen Ergebnissen nicht aufgefüllt. Verwenden Sie stattdessen das `Original` Feld.

Der Schweregrad des Ergebnisses berücksichtigt nicht den kritischen Charakter der beteiligten Komponenten oder der zugrunde liegenden Ressource. Der kritische Charakter ist definiert als die Wichtigkeit der Ressourcen, die mit dem Ergebnis verbunden sind. Beispielsweise hat eine Ressource, die einer geschäftskritischen Anwendung zugeordnet ist, eine höhere Priorität als eine Ressource, die nicht produktionstechnischen Tests zugeordnet ist. Verwenden Sie das `Criticality`-Feld, um Informationen zum kritischen Charakter der Ressource zu erfassen.

Wir empfehlen, bei der Übersetzung der systemeigenen Schweregrade der Ergebnisse in den Wert von im ASFF die folgenden Hinweise zu beachten. `Severity.Label`

- `INFORMATIONAL`— Diese Kategorie kann einen Befund für einen`PASSED`,`WARNING`, oder `NOT AVAILABLE` Scheck oder eine Identifizierung sensibler Daten beinhalten.
- `LOW`— Erkenntnisse, die zu future Kompromissen führen könnten. Zu dieser Kategorie können beispielsweise Sicherheitslücken, Konfigurationsschwächen und offengelegte Passwörter gehören.
- `MEDIUM`— Ergebnisse, die auf einen aktiven Kompromiss hindeuten, aber keinen Hinweis darauf, dass ein Gegner seine Ziele erreicht hat. Zu dieser Kategorie können beispielsweise Malware-Aktivitäten, Hacking-Aktivitäten und die Erkennung ungewöhnlicher Verhaltensweisen gehören.
- `HIGH`oder `CRITICAL` — Ergebnisse, die darauf hindeuten, dass ein Angreifer seine Ziele erreicht hat, wie z. B. aktiver Datenverlust oder Datenkompromittierung oder Denial-of-Service.

Beispiel

```
"Severity": {
    "Label": "CRITICAL",
    "Normalized": 90,
    "Original": "CRITICAL"
}
```

Title

Der Titel eines Fundes. Dieses Feld kann unspezifischen Standardtext oder spezifische Details für diese Instanz des Fundes enthalten.

Bei Kontrollergebnissen gibt dieses Feld den Titel der Kontrolle an.

Dieses Feld verweist nicht auf einen Standard, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

Beispiel

```
"Title": "AWS Config should be enabled"
```

Typen

Ein oder mehrere Fundtypen im Format *namespace*/*category*/*classifier*, die einen Fund klassifizieren. Dieses Feld verweist nicht auf einen Standard, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

`Types`sollte nur mit aktualisiert werden `BatchUpdateFindings`.

Wenn Sie nach Anbietern suchen, für die Sie einen Wert angeben möchten, `Types` sollten Sie das `Types` Attribut unter verwenden `FindingProviderFields`.

In der folgenden Liste sind die Aufzählungszeichen der obersten Ebene Namespaces, die Aufzählungszeichen der zweiten Ebene Kategorien und die Aufzählungszeichen der dritten Ebene Klassifikatoren. Wir empfehlen, dass Suchanbieter definierte Namespaces verwenden, um Ergebnisse zu sortieren und zu gruppieren. Die definierten Kategorien und Klassifikatoren können ebenfalls verwendet werden, sind aber nicht erforderlich. Nur der Software- und Konfigurationsprüfungs-Namespace hat definierte Klassifizierer.

Sie können einen Teilpfad für Namespace/Kategorie/Klassifikator definieren. Beispielsweise sind die folgenden Findungstypen alle gültig:

- TTPs
- TTPs/Defense Evasion
- ttps/Defense Evasion/ CloudTrailStopped

Die Kategorien Taktiken, Techniken und Verfahren (TTPs) in der folgenden Liste entsprechen der MITRE ATT&CK MatrixTM. Der Namespace Unusual Behaviors spiegelt allgemeines ungewöhnliches Verhalten wider, wie z. B. allgemeine statistische Anomalien, und ist nicht auf ein bestimmtes TTP abgestimmt. Sie könnten einen Fund jedoch mit beiden Fundtypen (Ungewöhnliches Verhalten und TTPs) klassifizieren.

Liste der Namespaces, Kategorien und Klassifikatoren:

- Software- und Konfigurationsprüfungen
  - Schwachstellen
    - CVE
  - AWS Bewährte Methoden im Bereich Sicherheit
    - Netzwerkerreichbarkeit
    - Laufzeitverhaltens-Analyse
  - Branchen- und regulatorische Standards
    - AWS Bewährte grundlegende Sicherheitsmethoden
    - CIS-Benchmarks zur Host-Härtung
    - Maßstab für AWS GUS-Stiftungen
    - PCI-DSS
    - Cloud Security Alliance-Kontrollen
    - ISO 90001-Kontrollen
    - ISO 27001-Kontrollen
    - ISO 27017-Kontrollen
    - ISO 27018-Kontrollen
    - SOC 1
    - SOC 2
    - HIPAA-Kontrollen (USA)
    - NIST 800-53-Kontrollen (USA)
    - NIST CSF-Kontrollen (USA)

    - IRAP-Kontrollen (Australien)
    - K-ISMS-Kontrollen (Korea)
    - MTCS-Kontrollen (Singapur)
    - FISC-Kontrollen (Japan)
    - My Number Act-Kontrollen (Japan)
    - ENS-Kontrollen (Spanien)
    - Cyber Essentials Plus-Kontrollen (Vereinigtes Königkreich)
    - G-Cloud-Kontrollen (Vereinigtes Königreich)
    - C5-Kontrollen (Deutschland)
    - IT-Grundschutz-Kontrollen (Deutschland)
    - DSGVO-Kontrollen (Europa)
    - TISAX-Kontrollen (Europa)
  - Patch-Management
- TTPs
  - Anfänglicher Zugriff
  - Ausführung
  - Persistenz
  - Rechteeskalation
  - Abwehrumgehung
  - Anmeldeinformationszugriff
  - Erkennung
  - Seitwärtsbewegung (Lateral Movement)
  - Sammlung
  - Command and Control
- Auswirkungen
  - Offenlegung von Daten
  - Datenexfiltration
  - Datenvernichtung
  - Denial of Service
  - Ressourcennutzung

- Ungewöhnliches Verhalten
  - Anwendung
  - Netzwerkfluss
  - IP-Adresse
  - Benutzer
  - VM
  - Container
  - Serverless
  - Prozess
  - Datenbank
  - Daten
- Identifizierung sensibler Daten
  - Personenbezogene Daten
  - Passwörter
  - Recht
  - Finanzanwendungen
  - Sicherheit
  - Geschäft

Beispiel

```
"Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
    ]
```

UpdatedAt

Gibt an, wann der Suchprovider den Suchdatensatz zuletzt aktualisiert hat.

Dieser Zeitstempel gibt den Zeitpunkt an, zu dem der Suchdatensatz zuletzt oder zuletzt aktualisiert wurde. Folglich kann er vom `LastObservedAt` Zeitstempel abweichen, der angibt, wann das Ereignis oder die Sicherheitsanfälligkeit zuletzt oder zuletzt beobachtet wurde.

Wenn Sie den Funddatensatz aktualisieren, müssen Sie diesen Zeitstempel durch den aktualisierten Zeitstempel ersetzen. Bei der Erstellung eines Befunddatensatzes müssen die Zeitstempel

`CreatedAt` und die `UpdatedAt` Zeitstempel identisch sein. Nach einer Aktualisierung des Suchdatensatzes muss der Wert dieses Felds aktueller sein als alle vorherigen Werte, die es enthielt.

Beachten Sie, dass dies `UpdatedAt` nicht mithilfe der `BatchUpdateFindings`API-Operation aktualisiert werden kann. Sie können es nur aktualisieren, indem Sie `BatchImportFindings`.

Beispiel

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

> **Note**
>
> Security Hub löscht Ergebnisse 90 Tage nach dem letzten Update oder 90 Tage nach dem Erstellungsdatum, wenn kein Update erfolgt. Um Ergebnisse länger als 90 Tage zu speichern, können Sie in Amazon eine Regel konfigurieren EventBridge , die Ergebnisse an Ihren S3-Bucket weiterleitet.

Optionale Attribute der obersten Ebene

Diese Attribute der obersten Ebene sind im AWS Security Finding Format (ASFF) optional. Weitere Informationen zu diesen Attributen finden Sie AwsSecurityFindingin der AWS Security Hub API-Referenz.

Aktion

Das `Action`Objekt enthält Details zu einer Aktion, die sich auf eine Ressource auswirkt oder die für eine Ressource ausgeführt wurde.

Beispiel

```
"Action": {
    "ActionType": "PORT_PROBE",
    "PortProbeAction": {
        "PortProbeDetails": [
            {
                "LocalPortDetails": {
                    "Port": 80,
                    "PortName": "HTTP"
                },
                "LocalIpDetails": {
```

```
                    "IpAddressV4": "192.0.2.0"
                },
                "RemoteIpDetails": {
                    "Country": {
                        "CountryName": "Example Country"
                    },
                    "City": {
                        "CityName": "Example City"
                    },
                    "GeoLocation": {
                        "Lon": 0,
                        "Lat": 0
                    },
                    "Organization": {
                        "AsnOrg": "ExampleASO",
                        "Org": "ExampleOrg",
                        "Isp": "ExampleISP",
                        "Asn": 64496
                    }
                }
            }
        ],
        "Blocked": false
    }
}
```

AwsAccountName

Der AWS-Konto Name, auf den sich das Ergebnis bezieht.

Beispiel

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

Der Name des Unternehmens für das Produkt, das zu dem Ergebnis geführt hat. Bei Ergebnissen, die auf Kontrollen beruhen, lautet das Unternehmen. AWS

Security Hub füllt dieses Attribut automatisch für jeden Befund aus. Sie können es nicht mit `BatchImportFindings` oder `BatchUpdateFindings` aktualisieren. Die Ausnahme ist, wenn Sie eine benutzerdefinierte Integration verwenden. Siehe the section called “Verwenden benutzerdefinierter Produktintegrationen”.

Wenn Sie die Security Hub Hub-Konsole verwenden, um Ergebnisse nach Firmennamen zu filtern, verwenden Sie dieses Attribut. Wenn Sie die Security Hub Hub-API verwenden, um Ergebnisse nach Firmennamen zu filtern, verwenden Sie das `aws/securityhub/CompanyName` Attribut unter`ProductFields`. Security Hub synchronisiert diese beiden Attribute nicht.

Beispiel

```
"CompanyName": "AWS"
```

-Compliance

Das `Compliance`Objekt enthält Suchdetails zu einem Steuerelement. Dieses Attribut wird für Ergebnisse zurückgegeben, die von einem Security Hub-Steuerelement generiert wurden, und für Ergebnisse, die AWS Config an Security Hub gesendet werden.

Beispiel

```
"Compliance": {
    "AssociatedStandards": [
        {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
        {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
        {"StandardsId": "standards/nist-800-53/v/5.0.0"}
    ],
    "RelatedRequirements": [
        "NIST.800-53.r5 AC-4",
        "NIST.800-53.r5 AC-4(21)",
        "NIST.800-53.r5 SC-7",
        "NIST.800-53.r5 SC-7(11)",
        "NIST.800-53.r5 SC-7(16)",
        "NIST.800-53.r5 SC-7(21)",
        "NIST.800-53.r5 SC-7(4)",
        "NIST.800-53.r5 SC-7(5)"
    ],
    "SecurityControlId": "EC2.18",
    "SecurityControlParameters":[
        {
            "Name": "authorizedTcpPorts",
            "Value": ["80", "443"]
        },
        {
            "Name": "authorizedUdpPorts",
            "Value": ["427"]
```

```
        }
    ],
    "Status": "NOT_AVAILABLE",
    "StatusReasons": [
        {
            "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
            "Description": "This finding has a compliance status of NOT AVAILABLE
 because AWS Config sent Security Hub a finding with a compliance state of Not
 Applicable. The potential reasons for a Not Applicable finding from Config are that
 (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has
 been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule
 itself includes scenarios where Not Applicable is returned. The specific reason why
 Not Applicable is returned is not available in the Config rule evaluation."
        }
    ]
}
```

Wahrscheinlichkeit

Die Wahrscheinlichkeit, dass ein Ergebnis das Verhalten oder das Problem, das identifiziert werden sollte, genau identifiziert.

`Confidence`sollte nur mit aktualisiert werden `BatchUpdateFindings`.

Wenn Sie nach Anbietern suchen, für die Sie einen Wert angeben möchten, `Confidence` sollten Sie das `Confidence` Attribut unter verwenden`FindingProviderFields`. Siehe the section called “Verwenden von FindingProviderFields”.

`Confidence`wird anhand einer Verhältnisskala auf einer Basis von 0—100 bewertet. 0 bedeutet 0 Prozent Konfidenz, und 100 bedeutet 100 Prozent Konfidenz. Beispielsweise hat eine Erkennung einer Datenexfiltration, die auf einer statistischen Abweichung des Netzwerkverkehrs basiert, eine geringe Zuverlässigkeit, da eine tatsächliche Exfiltration nicht verifiziert wurde.

Beispiel

```
"Confidence": 42
```

Kritikalität

Die Wichtigkeit, die den Ressourcen zugewiesen wird, die mit einem Ergebnis verknüpft sind.

`Criticality`sollte nur durch Aufrufen der `BatchUpdateFindings`API-Operation aktualisiert werden. Aktualisieren Sie dieses Objekt nicht mit `BatchImportFindings`.

Wenn Sie nach Anbietern suchen, für die Sie einen Wert angeben möchten, `Criticality` sollten Sie das `Criticality` Attribut unter verwenden`FindingProviderFields`. Siehe the section called “Verwenden von FindingProviderFields”.

`Criticality`wird auf einer Basis von 0—100 bewertet, wobei eine Verhältnisskala verwendet wird, die nur ganze Zahlen unterstützt. Ein Wert von 0 bedeutet, dass die zugrunde liegenden Ressourcen keine Kritikalität haben, und der Wert 100 ist den wichtigsten Ressourcen vorbehalten.

Beachten Sie bei der Zuweisung für jede Ressource Folgendes: `Criticality`

- Enthält die betroffene Ressource sensible Daten (z. B. einen S3-Bucket mit PII)?
- Ermöglicht die betroffene Ressource einem Angreifer, seinen Zugriff zu vertiefen oder seine Fähigkeiten zur Ausführung zusätzlicher bösartiger Aktivitäten auszuweiten (z. B. ein kompromittiertes Systemadministratorkonto)?
- Ist die Ressource ein geschäftskritisches Asset (z. B. ein wesentliches Unternehmenssystem, dessen Kompromittierung bedeutende Umsatzeinbußen verursachen könnte)?

Sie können die folgenden Richtlinien verwenden:

- Eine Ressource, die geschäftskritische Systeme mit Strom versorgt oder hochsensible Daten enthält, kann im Bereich von 75 bis 100 bewertet werden.
- Eine Ressource, die wichtige (aber nicht kritische Systeme) mit Strom versorgt oder mäßig wichtige Daten enthält, kann im Bereich 25—74 bewertet werden.
- Eine Ressource, die unwichtige Systeme unterstützt oder unsensible Daten enthält, sollte im Bereich von 0—24 bewertet werden.

Beispiel

```
"Criticality": 99
```

FindingProviderFields

`FindingProviderFields`umfasst die folgenden Attribute:

- `Confidence`
- `Criticality`
- `RelatedFindings`

- `Severity`
- `Types`

Sie können `FindingProviderFields` mithilfe der `BatchImportFindings`API-Operation aktualisieren. Sie können es nicht mit aktualisieren `BatchUpdateFindings`.

Einzelheiten darüber, wie Security Hub Updates von `BatchImportFindings`zu `FindingProviderFields` und zu den entsprechenden Attributen der obersten Ebene verarbeitet, finden Sie unterthe section called “Verwenden von FindingProviderFields”.

Beispiel

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

FirstObservedAt

Gibt an, wann das potenzielle Sicherheitsproblem, das durch einen Befund erkannt wurde, zum ersten Mal beobachtet wurde.

Dieser Zeitstempel gibt den Zeitpunkt an, zu dem das Ereignis oder die Sicherheitsanfälligkeit zum ersten Mal beobachtet wurde. Folglich kann er vom `CreatedAt` Zeitstempel abweichen, der den Zeitpunkt angibt, zu dem dieser Befunddatensatz erstellt wurde.

Dieser Zeitstempel sollte zwischen Aktualisierungen des Ergebnisdatensatzes unveränderlich sein, kann aber aktualisiert werden, wenn ein genauerer Zeitstempel bestimmt wird.

Beispiel

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

Gibt an, wann das potenzielle Sicherheitsproblem, das durch ein Ergebnis erkannt wurde, zuletzt vom Produkt mit Sicherheitsergebnissen festgestellt wurde.

Dieser Zeitstempel gibt den Zeitpunkt an, zu dem das Ereignis oder die Sicherheitsanfälligkeit zuletzt oder zuletzt beobachtet wurde. Folglich kann er vom `UpdatedAt` Zeitstempel abweichen, der angibt, wann dieser Ergebnisdatensatz zuletzt oder zuletzt aktualisiert wurde.

Sie können diesen Zeitstempel angeben, er ist jedoch bei der ersten Beobachtung nicht erforderlich. Wenn Sie dieses Feld bei der ersten Beobachtung angeben, sollte der Zeitstempel mit dem Zeitstempel identisch sein. `FirstObservedAt` Sie sollten dieses Feld immer wieder aktualisieren, sodass immer der Zeitstempel der letzten Beobachtung des Fundes angegeben wird.

Beispiel

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

Schadsoftware

Das Objekt `Malware` stellt eine Liste der Malware zur Verfügung, die mit einem Fund zusammenhängt.

Beispiel

```
"Malware": [
    {
        "Name": "Stringler",
        "Type": "COIN_MINER",
        "Path": "/usr/sbin/stringler",
        "State": "OBSERVED"
    }
]
```

Netzwerk (im Ruhestand)

Das `Network`Objekt stellt netzwerkbezogene Informationen zu einem Befund bereit.

Dieses Objekt ist ausgemustert. Um diese Daten bereitzustellen, können Sie die Daten entweder einer Ressource in zuordnen `Resources` oder das `Action` Objekt verwenden.

Beispiel

```
"Network": {
    "Direction": "IN",
    "OpenPortRange": {
        "Begin": 443,
        "End": 443
    },
    "Protocol": "TCP",
    "SourceIpV4": "1.2.3.4",
    "SourceIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "SourcePort": "42",
    "SourceDomain": "example1.com",
    "SourceMac": "00:0d:83:b1:c0:8e",
    "DestinationIpV4": "2.3.4.5",
    "DestinationIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "DestinationPort": "80",
    "DestinationDomain": "example2.com"
}
```

NetworkPath

Das `NetworkPath`Objekt stellt Informationen über einen Netzwerkpfad bereit, der mit einem Befund zusammenhängt. Jeder Eintrag in `NetworkPath` steht für eine Komponente des Pfads.

Beispiel

```
"NetworkPath" : [
    {
        "ComponentId": "abc-01a234bc56d8901ee",
        "ComponentType": "AWS::EC2::InternetGateway",
        "Egress": {
            "Destination": {
                "Address": [ "192.0.2.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                ]
```

```
            },
            "Protocol": "TCP",
            "Source": {
                "Address": ["203.0.113.0/24"]
            }
        },
        "Ingress": {
            "Destination": {
                "Address": [ "198.51.100.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                 ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": [ "203.0.113.0/24" ]
            }
        }
     }
]
```

Hinweis

Das `Note`Objekt gibt eine benutzerdefinierte Notiz an, die Sie zu einem Ergebnis hinzufügen können.

Ein Ergebnisanbieter kann eine erste Notiz für ein Ergebnis bereitstellen, aber danach können keine Notizen hinzugefügt werden. Sie können eine Notiz nur mit `BatchUpdateFindings`aktualisieren.

Beispiel

```
"Note": {
    "Text": "Don't forget to check under the mat.",
    "UpdatedBy": "jsmith",
    "UpdatedAt": "2018-08-31T00:15:09Z"
}
```

PatchSummary

Das `PatchSummary`Objekt bietet eine Zusammenfassung des Patch-Konformitätsstatus einer Instanz anhand eines ausgewählten Konformitätsstandards.

Beispiel

```
"PatchSummary" : {
    "FailedCount" : 0,
    "Id" : "pb-123456789098",
    "InstalledCount" : 100,
    "InstalledOtherCount" : 1023,
    "InstalledPendingReboot" : 0,
    "InstalledRejectedCount" : 0,
    "MissingCount" : 100,
    "Operation" : "Install",
    "OperationEndTime" : "2018-09-27T23:39:31Z",
    "OperationStartTime" : "2018-09-27T23:37:31Z",
    "RebootOption" : "RebootIfNeeded"
}
```

Prozess

Das `Process`Objekt enthält prozessbezogene Details zu einem Ergebnis.

Beispiel:

```
"Process": {
    "LaunchedAt": "2018-09-27T22:37:31Z",
    "Name": "syslogd",
    "ParentPid": 56789,
    "Path": "/usr/sbin/syslogd",
    "Pid": 12345,
    "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

Zeigt an, wann Security Hub ein Ergebnis erhalten hat und mit der Verarbeitung beginnt.

Dies unterscheidet sich von `CreatedAt` und`UpdatedAt`, bei denen es sich um erforderliche Zeitstempel handelt, die sich auf die Interaktion des Ermittlungsanbieters mit dem Sicherheitsproblem und dem Ergebnis beziehen. Der `ProcessedAt` Zeitstempel gibt an, wann Security Hub mit der Verarbeitung eines Ergebnisses beginnt. Ein Ergebnis wird nach Abschluss der Verarbeitung im Konto eines Benutzers angezeigt.

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

Ein Datentyp, bei dem Produkte mit Sicherheitsergebnissen zusätzliche lösungsspezifische Details enthalten können, die nicht Teil des definierten AWS Sicherheitsfindungsformats sind.

Für Ergebnisse, die durch Security Hub Hub-Kontrollen generiert wurden, `ProductFields` enthält dies Informationen über die Kontrolle. Siehe the section called “Generierung und Aktualisierung der Kontrollergebnisse”.

Dieses Feld sollte keine redundanten Daten enthalten und darf keine Daten enthalten, die mit Feldern im AWS Security Finding Format in Konflikt stehen.

Das Präfix `aws/` "" steht für einen reservierten Namespace, der nur für AWS Produkte und Dienstleistungen reserviert ist und darf nicht zusammen mit Ergebnissen aus Integrationen von Drittanbietern eingereicht werden.

Auch wenn dies nicht unbedingt erforderlich ist, sollten Produkte Feldnamen wir folgt formatieren: `company-id/product-id/field-name`. Dabei sollten die `company-id` und `product-id` den Angaben im `ProductArn` des Fundes entsprechen.

Die Felder, auf die verwiesen wird, `Archival` werden verwendet, wenn Security Hub ein vorhandenes Ergebnis archiviert. Security Hub archiviert beispielsweise vorhandene Ergebnisse, wenn Sie eine Kontrolle oder einen Standard deaktivieren und wenn Sie konsolidierte Kontrollergebnisse ein- oder ausschalten.

Dieses Feld kann auch Informationen über den Standard enthalten, der die Kontrolle beinhaltet, die zu dem Ergebnis geführt hat.

Beispiel

```
"ProductFields": {
    "API", "DeleteTrail",
    "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because
 consolidated control findings has been turned on or off. This causes findings in the
 previous state to be archived when new findings are being generated.",
    "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
    "aws/inspector/AssessmentTargetName": "My prod env",
    "aws/inspector/AssessmentTemplateName": "My daily CVE assessment",
    "aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",
    "generico/secure-pro/Action.Type", "AWS_API_CALL",
    "generico/secure-pro/Count": "6",
    "Service_Name": "cloudtrail.amazonaws.com"
```

```
}
```

ProductName

Gibt den Namen des Produkts an, das den Befund generiert hat. Für Ergebnisse, die auf Kontrollen basieren, lautet der Produktname Security Hub.

Security Hub füllt dieses Attribut automatisch für jeden Befund aus. Sie können es nicht mit `BatchImportFindings`oder `BatchUpdateFindings`aktualisieren. Die Ausnahme ist, wenn Sie eine benutzerdefinierte Integration verwenden. Siehe the section called “Verwenden benutzerdefinierter Produktintegrationen”.

Wenn Sie die Security Hub Hub-Konsole verwenden, um Ergebnisse nach Produktnamen zu filtern, verwenden Sie dieses Attribut.

Wenn Sie die Security Hub Hub-API verwenden, um Ergebnisse nach Produktnamen zu filtern, verwenden Sie das `aws/securityhub/ProductName` Attribut unter`ProductFields`.

Security Hub synchronisiert diese beiden Attribute nicht.

RecordState

Stellt den Datensatzstatus eines Ergebnisses bereit.

Standardmäßig werden Funde als `ACTIVE` erachtet, wenn sie anfangs von einem Service generiert werden.

Der Status `ARCHIVED` gibt an, dass ein Fund nicht mehr sichtbar sein sollte. Archivierte Ergebnisse werden nicht sofort gelöscht. Sie können nach ihnen suchen, sie überprüfen und darüber Bericht erstatten. Security Hub archiviert automatisch kontrollbasierte Ergebnisse, wenn die zugehörige Ressource gelöscht wird, die Ressource nicht existiert oder die Kontrolle deaktiviert ist.

`RecordState`ist für die Suche nach Anbietern vorgesehen und kann nur von aktualisiert werden. `BatchImportFindings` Sie können es nicht aktualisieren mit `BatchUpdateFindings`.

Um den Status Ihrer Untersuchung zu einem Ergebnis nachzuverfolgen, verwenden Sie `Workflow`stattRecordState.

Wenn sich der Datensatzstatus von `ARCHIVED` zu `ACTIVE` ändert und der Workflow-Status des Ergebnisses entweder `NOTIFIED` oder lautet`RESOLVED`, setzt Security Hub den Workflow-Status automatisch auf`NEW`.

Beispiel

```
"RecordState": "ACTIVE"
```

Region

Gibt das an, AWS-Region aus dem das Ergebnis generiert wurde.

Security Hub füllt dieses Attribut automatisch für jeden Befund aus. Sie können es nicht mit `BatchImportFindings` oder `BatchUpdateFindings` aktualisieren.

Beispiel

```
"Region": "us-west-2"
```

RelatedFindings

Stellt eine Liste von Ergebnissen bereit, die sich auf das aktuelle Ergebnis beziehen.

`RelatedFindings` sollte nur mit der `BatchUpdateFindings` API-Operation aktualisiert werden. Sie sollten dieses Objekt nicht mit aktualisieren `BatchImportFindings`.

Für `BatchImportFindings` Anfragen sollte die Suche nach Anbietern das `RelatedFindings` Objekt unter verwenden `FindingProviderFields`.

Beschreibungen der `RelatedFindings` Attribute finden Sie `RelatedFinding` in der AWS Security Hub API-Referenz.

Beispiel

```
"RelatedFindings": [
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000" },
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "AcmeNerfHerder-111111111111-x189dx7824" }
]
```

Abhilfe

Das Objekt `Remediation` enthält Informationen zu empfohlenen Behebungsschritten für das Problem.

Beispiel

```
"Remediation": {
    "Recommendation": {
        "Text": "For instructions on how to fix this issue, see the AWS Security Hub
 documentation for EC2.2.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"
    }
}
```

Beispiel

Gibt an, ob es sich bei dem Ergebnis um ein Beispielergebnis handelt.

```
"Sample": true
```

SourceUrl

Das `SourceUrl` Objekt stellt eine URL bereit, die auf eine Seite verweist, die sich mit dem aktuellen Ergebnis im gefundenen Produkt befasst.

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

Das `ThreatIntelIndicator`Objekt stellt Bedrohungsinformationen bereit, die sich auf einen Befund beziehen.

Beispiel

```
"ThreatIntelIndicators": [
  {
    "Category": "BACKDOOR",
    "LastObservedAt": "2018-09-27T23:37:31Z",
    "Source": "Threat Intel Weekly",
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",
    "Type": "IPV4_ADDRESS",
    "Value": "8.8.8.8",
  }
]
```

Bedrohungen

Das `Threats`Objekt enthält Details zu der Bedrohung, die durch einen Befund erkannt wurde.

Beispiel

```
"Threats": [{
    "FilePaths": [{
        "FileName": "b.txt",
        "FilePath": "/tmp/b.txt",
        "Hash": "sha256",
        "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"
    }],
    "ItemCount": 3,
    "Name": "Iot.linux.mirai.vwisi",
    "Severity": "HIGH"
}]
```

UserDefinedFields

Stellt eine Liste von Zeichenfolgenpaaren aus Name und Wert bereit, die dem Befund zugeordnet sind. Dies sind individuelle, benutzerdefinierte Felder, die einem Fund hinzugefügt werden. Diese Felder können anhand Ihrer spezifischen Konfiguration automatisch generiert werden.

Bei der Suche nach Anbietern sollte dieses Feld nicht für Daten verwendet werden, die das Produkt generiert. Stattdessen kann das `ProductFields` Feld bei der Suche nach Anbietern für Daten verwendet werden, die keinem Standardfeld im Format für AWS Sicherheitssuche zugeordnet sind.

Diese Felder können nur mit `BatchUpdateFindings` aktualisiert werden.

Beispiel

```
"UserDefinedFields": {
    "reviewedByCio": "true",
    "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

Stellt den Wahrheitsgehalt eines Ergebnisses sicher. Finds-Produkte können `UNKNOWN` für dieses Feld einen Wert von angeben. Ein Ergebnisprodukt sollte einen Wert für dieses Feld liefern, wenn das System des Ergebnisprodukts ein aussagekräftiges Analogon enthält. Dieses Feld wird in der Regel durch eine Benutzerentscheidung oder eine Aktion nach der Untersuchung eines Ergebnisses gefüllt.

Ein Ergebnisanbieter kann einen Anfangswert für dieses Attribut bereitstellen, es danach aber nicht aktualisieren. Sie können dieses Attribut nur aktualisieren, indem Sie `BatchUpdateFindings`

```
"VerificationState": "Confirmed"
```

Schwachstellen

Das `Vulnerabilities`Objekt enthält eine Liste von Sicherheitslücken, die mit einem Befund verknüpft sind.

Beispiel

```
"Vulnerabilities" : [
    {
        "CodeVulnerabilities": [{
            "Cwes": [
                "CWE-798",
                "CWE-799"
            ],
            "FilePath": {
                "EndLine": 421,
                "FileName": "package-lock.json",
                "FilePath": "package-lock.json",
                "StartLine": 420
            },
                "SourceArn":"arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-
Extension:114"
        }],
        "Cvss": [
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
                "Version": "V3"
            },
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
                "Version": "V2"
            }
        ],
        "EpssScore": 0.015,
        "ExploitAvailable": "YES",
        "FixAvailable": "YES",
```

```
        "Id": "CVE-2020-12345",
        "LastKnownExploitAt": "2020-01-16T00:01:35Z",
        "ReferenceUrls":[
           "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",
            "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
        ],
        "RelatedVulnerabilities": ["CVE-2020-12345"],
        "Vendor": {
            "Name": "Alas",
            "Url":"https://alas.aws.amazon.com/ALAS-2020-1337.html",
            "VendorCreatedAt":"2020-01-16T00:01:43Z",
            "VendorSeverity":"Medium",
            "VendorUpdatedAt":"2020-01-16T00:01:43Z"
        },
        "VulnerablePackages": [
            {
                "Architecture": "x86_64",
                "Epoch": "1",
                "FilePath": "/tmp",
                "FixedInVersion": "0.14.0",
                "Name": "openssl",
                "PackageManager": "OS",
                "Release": "16.amzn2.0.3",
                "Remediation": "Update aws-crt to 0.14.0",
                "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
                "SourceLayerHash":
 "sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
                "Version": "1.0.2k"
            }
        ]
    }
]
```

Workflow

Das `Workflow`-Objekt bietet Informationen über den Status der Untersuchung zu einem Ergebnis.

Dieses Feld ist für Kunden zur Verwendung mit Tools zur Problembehebung, Orchestrierung und Ticketausstellung vorgesehen. Es ist nicht für die Suche nach Anbietern bestimmt.

Sie können das Feld nur mit aktualisieren. `Workflow` `BatchUpdateFindings` Kunden können ihn auch über die Konsole aktualisieren. Siehe the section called “Den Workflow-Status von Ergebnissen festlegen”.

Beispiel

```
"Workflow": {
    "Status": "NEW"
}
```

WorkflowState (Im Ruhestand)

Dieses Objekt ist ausgemustert und wurde durch das `Status` Feld des `Workflow` Objekts ersetzt.

Dieses Feld gibt den Workflow-Status eines Ergebnisses an. Funde generierende Produkte können in diesem Feld den Wert `NEW` angeben. Ein Funde generierendes Produkte kann einen Wert in diesem Feld angeben, wenn es ein aussagekräftiges Analogon im System des Produkts gibt.

Beispiel

```
"WorkflowState": "NEW"
```

Resources

Das Objekt `Resources` stellt Informationen zu den Ressourcen bereit, die an einem Fund beteiligt sind.

Es enthält ein Array von bis zu 32 Ressourcenobjekten.

Informationen zur Formatierung von Ressourcennamen finden Sie unterAWS Syntax des Security Finding Format (ASFF).

Beispiele für jedes Ressourcenobjekt finden Sie in der folgenden Liste.

Themen

- Ressourcenattribute
- AwsAmazonMQ
- AwsApiGateway
- AwsAppSync
- AwsAthena
- AwsAutoScaling
- AwsBackup

- AwsCertificateManager
- AwsCloudFormation
- AwsCloudFront
- AwsCloudTrail
- AwsCloudWatch
- AwsCodeBuild
- AwsDms
- AwsDynamoDB
- AwsEc2
- AwsEcr
- AwsEcs
- AwsEfs
- AwsEks
- AwsElasticBeanstalk
- AwsElasticSearch
- AwsElb
- AwsEventBridge
- AwsGuardDuty
- AwsIam
- AwsKinesis
- AwsKms
- AwsLambda
- AwsMsk
- AwsNetworkFirewall
- AwsOpenSearchService
- AwsRds
- AwsRedshift
- AwsRoute53
- AwsS3
- AwsSageMaker

- AwsSecretsManager
- AwsSns
- AwsSqs
- AwsSsm
- AwsStepFunctions
- AwsWaf
- AwsXray
- Container
- Other

Ressourcenattribute

Hier finden Sie Beschreibungen und Beispiele für das `Resources` Objekt im AWS Security Finding Format (ASFF). Weitere Informationen zu diesen Feldern finden Sie unter Ressourcen.

ApplicationArn

Identifiziert den Amazon-Ressourcennamen (ARN) der Anwendung, die an der Entdeckung beteiligt war.

Beispiel

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0"
```

ApplicationName

Identifiziert den Namen der Anwendung, die an der Entdeckung beteiligt war.

Beispiel

```
"ApplicationName": "SampleApp"
```

DataClassification

Das DataClassificationFeld enthält Informationen über vertrauliche Daten, die auf der Ressource erkannt wurden.

Beispiel

```
"DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
                        "Occurrences": {
                            "Pages": [
                                {
                                    "PageNumber": 1,
                                    "OffsetRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                     },
```

```
                                "LineRange": {
                                    "Start": 1,
                                    "End": 100,
                                    "StartColumn": 10
                                }
                            }
                        ]
                    }
                },
                {
                    "Count": 2229,
                    "Type": "URL",
                    "Occurrences": {
                       "LineRanges": [
                           {
                               "Start": 1,
                               "End": 13
                           }
                       ]
                    }
                },
                {
                    "Count": 13826,
                    "Type": "NameDetection",
                    "Occurrences": {
                        "Records": [
                            {
                                "RecordIndex": 1,
                                "JsonPath": "$.ssn.value"
                            }
                        ]
                    }
                },
                {
                    "Count": 32,
                    "Type": "AddressDetection"
                }
            ],
            "TotalCount": 32
        }
    ],
    "CustomDataIdentifiers": {
        "Detections": [
            {
```

```
                    "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                    "Name": "1712be25e7c7f53c731fe464f1c869b8",
                    "Count": 2,
                }
            ],
            "TotalCount": 2
        }
    }
}
```

Details

Das Details Feld enthält zusätzliche Informationen über eine einzelne Ressource, die die entsprechenden Objekte verwendet. Jede Ressource muss in einem separaten Ressourcenobjekt im `Resources` Objekt bereitgestellt werden.

Beachten Sie, dass das `Details` Objekt aus dem Ergebnis entfernt wird, wenn die Ergebnisgröße das Maximum von 240 KB überschreitet. Für Kontrollergebnisse, die AWS Config Regeln verwenden, können Sie sich die Ressourcendetails in der AWS Config Konsole ansehen.

Security Hub bietet eine Reihe verfügbarer Ressourcendetails für die unterstützten Ressourcentypen. Diese Details entsprechen den Werten des `Type` Objekts. Verwenden Sie nach Möglichkeit die bereitgestellten Typen.

Wenn es sich bei der Ressource beispielsweise um einen S3-Bucket handelt, legen Sie die Ressource `Type` auf fest `AwsS3Bucket` und geben Sie die Ressourcendetails im `AwsS3Bucket` Objekt an.

Mit dem `Other` Objekt können Sie benutzerdefinierte Felder und Werte angeben. Sie verwenden das `Other` Objekt in den folgenden Fällen:

- Der Ressourcentyp (der Wert der ResourceType) hat kein entsprechendes Detailobjekt. Um Details für die Ressource bereitzustellen, verwenden Sie das `Other` Objekt.
- Das Objekt für den Ressourcentyp enthält nicht alle Felder, die Sie auffüllen möchten. Verwenden Sie in diesem Fall das Detailobjekt für den Ressourcentyp, um die verfügbaren Felder auszufüllen. Verwenden Sie das `Other` Objekt, um die Felder aufzufüllen, die sich nicht im typspezifischen Objekt befinden.
- Der Ressourcentyp gehört nicht zu den angegebenen Typen. Stellen Sie in diesem Fall `Resource.Type` auf ein und verwenden Sie das `Other` Objekt`Other`, um die Details aufzufüllen.

Beispiel

```
"Details": {
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IpV4Addresses": ["1.1.1.1"],
    "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    },
    "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
    ],
    "SubnetId": "PublicSubnet",
    "Type": "i3.xlarge",
    "VirtualizationType": "hvm",
    "VpcId": "TestVPCIpv6"
  },
  "AwsS3Bucket": {
    "OwnerId": "da4d66eac431652a4d44d490a00500bded52c97d235b7b4752f9f688566fe6de",
    "OwnerName": "acmes3bucketowner"
  },
  "Other": { "LightPen": "blinky", "SerialNo": "1234abcd"}
}
```

Id

Der Bezeichner für den angegebenen Ressourcentyp.

Für AWS Ressourcen, die durch Amazon Resource Names (ARNs) identifiziert werden, ist dies der ARN.

Für AWS Ressourcen, denen ARNs fehlen, ist dies die Kennung, wie sie von dem AWS Service definiert wurde, der die Ressource erstellt hat.

Bei AWS Nicht-Ressourcen ist dies eine eindeutige Kennung, die der Ressource zugeordnet ist.

Beispiel

```
"Id": "arn:aws:s3:::example-bucket"
```

Partition

Die Partition, in der sich die Ressource befindet. Eine Partition ist eine Gruppe von AWS-Regionen. Jede AWS-Konto ist auf eine Partition beschränkt.

Die folgenden Partitionen werden unterstützt:

- `aws` – AWS-Regionen
- `aws-cn` – China-Regionen
- `aws-us-gov` – AWS GovCloud (US) Region

Beispiel

```
"Partition": "aws"
```

Region

Der Code für den AWS-Region Ort, an dem sich diese Ressource befindet. Eine Liste der Regionscodes finden Sie unter Regionale Endpunkte.

Beispiel

```
"Region": "us-west-2"
```

ResourceRole

Identifiziert die Rolle der Ressource bei dem Ergebnis. Eine Ressource ist entweder das Ziel der Suchaktivität oder der Akteur, der die Aktivität ausgeführt hat.

Beispiel

```
"ResourceRole": "target"
```

Tags

Sie können Ressourcen-Tags zu Ergebnissen hinzufügen, die in Security Hub aufgenommen werden, einschließlich Ergebnissen aus integrierten Produkten AWS-Services und Produkten von Drittanbietern. Sie können Ressourcen taggen, die vom `GetResources` Betrieb der AWS Resource Groups Tagging-API unterstützt werden. Eine Liste der unterstützten Ressourcen finden Sie unter Dienste, die die Resource Groups Tagging API unterstützen.

Beim Hinzufügen von Tags erfahren Sie, welche Tags einer Ressource zum Zeitpunkt der Verarbeitung des Ergebnisses zugeordnet waren. Sie können das `Tags` Attribut nur für Ressourcen einbeziehen, denen ein Tag zugeordnet ist. Wenn eine Ressource keine zugeordneten Tags hat, beziehen Sie beim Fund kein `Tags`-Attribut mit ein.

Durch die Aufnahme von Ressourcen-Tags in die Ergebnisse entfällt die Notwendigkeit, Pipelines zur Datenanreicherung zu erstellen oder die Metadaten von Sicherheitsergebnissen manuell anzureichern. Sie können Tags auch verwenden, um Ergebnisse und Erkenntnisse zu suchen oder zu filtern und Automatisierungsregeln zu erstellen.

Informationen zu Einschränkungen, die für Tags gelten, finden Sie unter Einschränkungen und Anforderungen für die Benennung von Tags.

In diesem Feld können Sie nur Tags angeben, die auf einer AWS Ressource vorhanden sind. Verwenden Sie das Unterfeld „`Other`Details“, um Daten bereitzustellen, die nicht im AWS Security Finding Format definiert sind.

Beispiel

```
"Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": "true"
}
```

Typ

Der Ressourcentyp, für den Sie Details angeben.

Verwenden Sie nach Möglichkeit einen der bereitgestellten Ressourcentypen, z. B. `AwsEc2Instance` oder `AwsS3Bucket`.

Wenn der Ressourcentyp keinem der angegebenen Ressourcentypen entspricht, legen Sie die Ressource `Type` auf `Other` fest und füllen Sie die `Other` Details im Unterfeld „Details“ aus.

Unterstützte Werte sind unter Ressourcen aufgeführt.

Beispiel

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQ

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format (ASFF) für `AwsAmazonMQ` Ressourcen.

AwsAmazonMQBroker

`AwsAmazonMQBroker`bietet Informationen über einen Amazon MQ-Broker, eine Message-Broker-Umgebung, die auf Amazon MQ ausgeführt wird.

Das folgende Beispiel zeigt den ASFF für das Objekt. `AwsAmazonMQBroker` Beschreibungen von `AwsAmazonMQBroker` Attributen finden Sie unter AwsAmazonMQBroker in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsAmazonMQBroker": {
    "AutoMinorVersionUpgrade": true,
    "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerName": "TestBroker",
    "Configuration": {
        "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "Revision": 1
    },
    "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
    "EncryptionOptions": {
        "UseAwsOwnedKey": true
    },
    "EngineType": "ActiveMQ",
    "EngineVersion": "5.17.2",
    "HostInstanceType": "mq.t2.micro",
    "Logs": {
        "Audit": false,
        "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/
audit",
```

```
        "General": false,
        "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111/general"
    },
    "MaintenanceWindowStartTime": {
        "DayOfWeek": "MONDAY",
        "TimeOfDay": "22:00",
        "TimeZone": "UTC"
    },
    "PubliclyAccessible": true,
    "SecurityGroups": [
        "sg-021345abcdef6789"
    ],
    "StorageType": "efs",
    "SubnetIds": [
        "subnet-1234567890abcdef0",
        "subnet-abcdef01234567890"
    ],
    "Users": [
        {
            "Username": "admin"
        }
    ]
}
```

AwsApiGateway

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsApiGateway` Ressourcen.

AwsApiGatewayRestApi

Das `AwsApiGatewayRestApi` Objekt enthält Informationen über eine REST-API in Version 1 von Amazon API Gateway.

Im Folgenden finden Sie ein Beispiel für einen `AwsApiGatewayRestApi` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsApiGatewayRestApi` Attribute finden Sie AwsApiGatewayRestApiDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
AwsApiGatewayRestApi: {
    "Id": "exampleapi",
```

```
    "Name": "Security Hub",
    "Description": "AWS Security Hub",
    "CreatedDate": "2018-11-18T10:20:05-08:00",
    "Version": "2018-10-26",
    "BinaryMediaTypes" : ["-'*~1*'"],
    "MinimumCompressionSize": 1024,
    "ApiKeySource": "AWS_ACCOUNT_ID",
    "EndpointConfiguration": {
        "Types": [
            "REGIONAL"
        ]
    }
}
```

AwsApiGatewayStage

Das `AwsApiGatewayStage` Objekt stellt Informationen zu einer Amazon API Gateway Gateway-Stufe der Version 1 bereit.

Im Folgenden finden Sie ein Beispiel für einen `AwsApiGatewayStage` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsApiGatewayStage` Attribute finden Sie AwsApiGatewayStageDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsApiGatewayStage": {
    "DeploymentId": "n7hlmf",
    "ClientCertificateId": "a1b2c3",
    "StageName": "Prod",
    "Description" : "Stage Description",
    "CacheClusterEnabled": false,
    "CacheClusterSize" : "1.6",
    "CacheClusterStatus": "NOT_AVAILABLE",
    "MethodSettings": [
        {
            "MetricsEnabled": true,
            "LoggingLevel": "INFO",
            "DataTraceEnabled": false,
            "ThrottlingBurstLimit": 100,
            "ThrottlingRateLimit": 5.0,
            "CachingEnabled": false,
            "CacheTtlInSeconds": 300,
            "CacheDataEncrypted": false,
```

```
            "RequireAuthorizationForCacheControl": true,
            "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
            "HttpMethod": "POST",
            "ResourcePath": "/echo"
        }
    ],
    "Variables": {"test": "value"},
    "DocumentationVersion": "2.0",
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "CanarySettings": {
        "PercentTraffic": 0.0,
        "DeploymentId": "ul73s8",
        "StageVariableOverrides" : [
            "String" : "String"
        ],
        "UseStageCache": false
    },
    "TracingEnabled": false,
    "CreatedDate": "2018-07-11T10:55:18-07:00",
    "LastUpdatedDate": "2020-08-26T11:51:04-07:00",
    "WebAclArn" : "arn:aws:waf-regional:us-west-2:111122223333:webacl/
cb606bd8-5b0b-4f0b-830a-dd304e48a822"
}
```

AwsApiGatewayV2Api

Das `AwsApiGatewayV2Api` Objekt enthält Informationen über eine API der Version 2 in Amazon API Gateway.

Im Folgenden finden Sie ein Beispiel für einen `AwsApiGatewayV2Api` Befund im AWS Security Finding Format (ASFF). Beschreibungen von `AwsApiGatewayV2Api` Attributen finden Sie unter AwsApiGatewayV2 ApiDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsApiGatewayV2Api": {
    "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
    "CreatedDate": "2020-03-28T00:32:37Z",
   "Description": "ApiGatewayV2 Api",
   "Version": "string",
    "Name": "my-api",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path",
   "CorsConfiguration": {
        "AllowOrigins": [ "*" ],
        "AllowCredentials": true,
        "ExposeHeaders": [ "string" ],
        "MaxAge": 3000,
        "AllowMethods": [
          "GET",
          "PUT",
          "POST",
          "DELETE",
          "HEAD"
        ],
        "AllowHeaders": [ "*" ]
    }
}
```

AwsApiGatewayV2-Stufe

`AwsApiGatewayV2Stage`enthält Informationen über eine Version 2-Stufe für Amazon API Gateway.

Im Folgenden finden Sie ein Beispiel für einen `AwsApiGatewayV2Stage` Befund im AWS Security Finding Format (ASFF). Beschreibungen von `AwsApiGatewayV2Stage` Attributen finden Sie unter AwsApiGatewayV2 StageDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsApiGatewayV2Stage": {
    "CreatedDate": "2020-04-08T00:36:05Z",
    "Description" : "ApiGatewayV2",
    "DefaultRouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "DeploymentId": "x1zwyv",
    "LastUpdatedDate": "2020-04-08T00:36:13Z",
    "RouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "StageName": "prod",
    "StageVariables": [
        "function": "my-prod-function"
    ],
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
```

```
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "AutoDeploy": false,
    "LastDeploymentStatusMessage": "Message",
    "ApiGatewayManaged": true,
}
```

AwsAppSync

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format (ASFF) für `AwsAppSync` Ressourcen.

AwsAppSyncGraphQLApi

`AwsAppSyncGraphQLApi`bietet Informationen über eine AWS AppSync GraphQL-API, bei der es sich um ein Konstrukt der obersten Ebene für Ihre Anwendung handelt.

Das folgende Beispiel zeigt den ASFF für das Objekt. `AwsAppSyncGraphQLApi` Beschreibungen von *`AwsAppSyncGraphQLApi`* Attributen finden Sie unter AwsAppSyncGraphQLApi in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsAppSyncGraphQLApi": {
    "AdditionalAuthenticationProviders": [
    {
     "AuthenticationType": "AWS_LAMBDA",
     "LambdaAuthorizerConfig": {
      "AuthorizerResultTtlInSeconds": 300,
      "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
     }
    },
    {
     "AuthenticationType": "AWS_IAM"
    }
    ],
    "ApiId": "021345abcdef6789",
    "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
    "AuthenticationType": "API_KEY",
    "Id": "021345abcdef6789",
```

```
    "LogConfig": {
     "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-
graphqlapi-logs-eu-central-1",
     "ExcludeVerboseContent": true,
     "FieldLogLevel": "ALL"
    },
    "Name": "My AppSync App",
    "XrayEnabled": true,
}
```

AwsAthena

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format (ASFF) für `AwsAthena` Ressourcen.

AwsAthenaWorkGroup

`AwsAthenaWorkGroup`bietet Informationen über eine Amazon Athena Athena-Arbeitsgruppe. Eine Arbeitsgruppe hilft Ihnen dabei, Benutzer, Teams, Anwendungen oder Workloads voneinander zu trennen. Sie hilft Ihnen auch dabei, Grenzen für die Datenverarbeitung festzulegen und die Kosten nachzuverfolgen.

Das folgende Beispiel zeigt den ASFF für das `AwsAthenaWorkGroup` Objekt. Beschreibungen der `AwsAthenaWorkGroup` Attribute finden Sie AwsAthenaWorkGroupin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsAthenaWorkGroup": {
    "Description": "My workgroup for prod workloads",
    "Name": "MyWorkgroup",
    "WorkgroupConfiguration" {
        "ResultConfiguration": {
            "EncryptionConfiguration": {
                "EncryptionOption": "SSE_KMS",
                "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
            }
        }
    },
        "State": "ENABLED"
}
```

AwsAutoScaling

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsAutoScaling` Ressourcen.

AwsAutoScalingAutoScalingGroup

Das `AwsAutoScalingAutoScalingGroup` Objekt enthält Details zu einer automatischen Skalierungsgruppe.

Im Folgenden finden Sie ein Beispiel für einen `AwsAutoScalingAutoScalingGroup` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsAutoScalingAutoScalingGroup` Attribute finden Sie AwsAutoScalingAutoScalingGroupDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsAutoScalingAutoScalingGroup": {
        "CreatedTime": "2017-10-17T14:47:11Z",
        "HealthCheckGracePeriod": 300,
        "HealthCheckType": "EC2",
        "LaunchConfigurationName": "mylaunchconf",
        "LoadBalancerNames": [],
        "LaunchTemplate": {
            "LaunchTemplateId": "string",
            "LaunchTemplateName": "string",
            "Version": "string"
        },
        "MixedInstancesPolicy": {
            "InstancesDistribution": {
                "OnDemandAllocationStrategy": "prioritized",
                "OnDemandBaseCapacity": number,
                "OnDemandPercentageAboveBaseCapacity": number,
                "SpotAllocationStrategy": "lowest-price",
                "SpotInstancePools": number,
                "SpotMaxPrice": "string"
            },
            "LaunchTemplate": {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "string",
                    "LaunchTemplateName": "string",
                    "Version": "string"
```

```
                },
                "CapacityRebalance": true,
                "Overrides": [
                    {
                       "InstanceType": "string",
                       "WeightedCapacity": "string"
                    }
                ]
            }
        }
    }
}
```

AwsAutoScalingLaunchConfiguration

Das `AwsAutoScalingLaunchConfiguration` Objekt enthält Details zu einer Startkonfiguration.

Im Folgenden finden Sie ein Beispiel für einen `AwsAutoScalingLaunchConfiguration` Befund im AWS Security Finding Format (ASFF).

Beschreibungen der `AwsAutoScalingLaunchConfiguration` Attribute finden Sie AwsAutoScalingLaunchConfigurationDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
AwsAutoScalingLaunchConfiguration: {
    "LaunchConfigurationName": "newtest",
    "ImageId": "ami-058a3739b02263842",
    "KeyName": "55hundredinstance",
    "SecurityGroups": [ "sg-01fce87ad6e019725" ],
    "ClassicLinkVpcSecurityGroups": [],
    "UserData": "...Base64-Encoded user data..."
    "InstanceType": "a1.metal",
    "KernelId": "",
    "RamdiskId": "ari-a51cf9cc",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/sdh",
            "Ebs": {
                "VolumeSize": 30,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true,
```

```
                "SnapshotId": "snap-ffaa1e69",
                "VirtualName": "ephemeral1"
            }
        },
        {
            "DeviceName": "/dev/sdb",
            "NoDevice": true
        },
        {
            "DeviceName": "/dev/sda1",
            "Ebs": {
                "SnapshotId": "snap-02420cd3d2dea1bc0",
                "VolumeSize": 8,
                "VolumeType": "gp2",
                "DeleteOnTermination": true,
                "Encrypted": false
            }
        },
        {
            "DeviceName": "/dev/sdi",
            "Ebs": {
                "VolumeSize": 20,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true
            }
        },
        {
            "DeviceName": "/dev/sdc",
            "NoDevice": true
        }
    ],
    "InstanceMonitoring": {
        "Enabled": false
    },
    "CreatedTime": 1620842933453,
    "EbsOptimized": false,
    "AssociatePublicIpAddress": true,
    "SpotPrice": "0.045"
}
```

AwsBackup

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsBackup` Ressourcen.

AwsBackupBackupPlan

Das `AwsBackupBackupPlan` Objekt stellt Informationen zu einem AWS Backup Backup-Plan bereit. Ein AWS Backup Backup-Plan ist ein Richtlinienausdruck, der definiert, wann und wie Sie Ihre AWS Ressourcen sichern möchten.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsBackupBackupPlan` Objekt. Beschreibungen der `AwsBackupBackupPlan` Attribute finden Sie AwsBackupBackupPlanin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsBackupBackupPlan": {
    "BackupPlan": {
     "AdvancedBackupSettings": [{
      "BackupOptions": {
       "WindowsVSS":"enabled"
      },
      "ResourceType":"EC2"
     }],
     "BackupPlanName": "test",
     "BackupPlanRule": [{
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "DailyBackups",
      "ScheduleExpression": "cron(0 5 ? * * *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
      },
      {
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
```

```
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "Monthly",
      "ScheduleExpression": "cron(0 5 1 * ? *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
     }]
    },
    "BackupPlanArn": "arn:aws:backup:us-east-1:858726136373:backup-
plan:b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "BackupPlanId": "b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "VersionId": "ZDVjNDIzMjItYTZiNS00NzczLTg4YzctNmExMWM2NjZhY2E1"
}
```

AwsBackupBackupVault

Das `AwsBackupBackupVault` Objekt stellt Informationen zu einem AWS Backup Backup-Tresor bereit. Ein AWS Backup Backup-Tresor ist ein Container, der Ihre Backups speichert und organisiert.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsBackupBackupVault` Objekt. Beschreibungen der `AwsBackupBackupVault` Attribute finden Sie AwsBackupBackupVaultin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsBackupBackupVault": {
    "AccessPolicy": {
     "Statement": [{
      "Action": [
       "backup:DeleteBackupVault",
       "backup:DeleteBackupVaultAccessPolicy",
       "backup:DeleteRecoveryPoint",
       "backup:StartCopyJob",
       "backup:StartRestoreJob",
       "backup:UpdateRecoveryPointLifecycle"
```

```
      ],
      "Effect": "Deny",
      "Principal": {
       "AWS": "*"
      },
      "Resource": "*"
     }],
     "Version": "2012-10-17"
    },
    "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/
automatic-backup-vault",
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "EncrytionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "Notifications": {
     "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED",
 "COPY_JOB_STARTED"],
     "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
    }
}
```

AwsBackupRecoveryPoint

Das `AwsBackupRecoveryPoint` Objekt stellt Informationen zu einer AWS Backup Sicherung bereit, die auch als Wiederherstellungspunkt bezeichnet wird. Ein AWS Backup Wiederherstellungspunkt stellt den Inhalt einer Ressource zu einem bestimmten Zeitpunkt dar.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsBackupRecoveryPoint` Objekt. Beschreibungen der `AwsBackupBackupVault` Attribute finden Sie AwsBackupRecoveryPointin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsBackupRecoveryPoint": {
    "BackupSizeInBytes": 0,
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "BackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/
automatic-backup-vault",
    "CalculatedLifecycle": {
     "DeleteAt": "2021-08-30T06:51:58.271Z",
     "MoveToColdStorageAt": "2020-08-10T06:51:58.271Z"
    },
    "CompletionDate": "2021-07-26T07:21:40.361Z",
```

```
    "CreatedBy": {
     "BackupPlanArn": "arn:aws:backup:us-east-1:111122223333:backup-plan:aws/
efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanId": "aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanVersion": "ZGM4YzY5YjktMWYxNC00ZTBmLWE5MjYtZmU5OWNiZmM5ZjIz",
     "BackupRuleId": "2a600c2-42ad-4196-808e-084923ebfd25"
    },
    "CreationDate": "2021-07-26T06:51:58.271Z",
    "EncryptionKeyArn": "arn:aws:kms:us-east-1:111122223333:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "IamRoleArn": "arn:aws:iam::111122223333:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup",
    "IsEncrypted": true,
    "LastRestoreTime": "2021-07-26T06:51:58.271Z",
    "Lifecycle": {
     "DeleteAfterDays": 35,
     "MoveToColdStorageAfterDays": 15
    },
    "RecoveryPointArn": "arn:aws:backup:us-east-1:111122223333:recovery-point:151a59e4-
f1d5-4587-a7fd-0774c6e91268",
    "ResourceArn": "arn:aws:elasticfilesystem:us-east-1:858726136373:file-system/
fs-15bd31a1",
    "ResourceType": "EFS",
    "SourceBackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/
efs/automatic-backup-vault",
    "Status": "COMPLETED",
    "StatusMessage": "Failure message",
    "StorageClass": "WARM"
}
```


AwsCertificateManager

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsCertificateManager` Ressourcen.

AwsCertificateManagerCertificate

Das `AwsCertificateManagerCertificate` Objekt enthält Details zu einem AWS Certificate Manager (ACM-) Zertifikat.

Im Folgenden finden Sie ein Beispiel für einen `AwsCertificateManagerCertificate` Befund im AWS Security Finding Format (ASFF). Beschreibungen

der `AwsCertificateManagerCertificate` Attribute finden Sie AwsCertificateManagerCertificateDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsCertificateManagerCertificate": {
    "CertificateAuthorityArn": "arn:aws:acm:us-west-2:444455556666:certificate-
authority/example",
    "CreatedAt": "2019-05-24T18:12:02.000Z",
    "DomainName": "example.amazondomains.com",
    "DomainValidationOptions": [
        {
            "DomainName": "example.amazondomains.com",
            "ResourceRecord": {
                "Name": "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                "Type": "CNAME",
                "Value": "_example.acm-validations.aws."
             },
             "ValidationDomain": "example.amazondomains.com",
             "ValidationEmails": [sample_email@sample.com],
             "ValidationMethod": "DNS",
             "ValidationStatus": "SUCCESS"
        }
    ],
    "ExtendedKeyUsages": [
        {
            "Name": "TLS_WEB_SERVER_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.1"
        },
        {
            "Name": "TLS_WEB_CLIENT_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.2"
        }
    ],
    "FailureReason": "",
    "ImportedAt": "2018-08-17T00:13:00.000Z",
    "InUseBy": ["arn:aws:amazondomains:us-west-2:444455556666:loadbalancer/example"],
    "IssuedAt": "2020-04-26T00:41:17.000Z",
    "Issuer": "Amazon",
    "KeyAlgorithm": "RSA-1024",
    "KeyUsages": [
        {
            "Name": "DIGITAL_SIGNATURE",
        },
```

```
        {
            "Name": "KEY_ENCIPHERMENT",
        }
    ],
    "NotAfter": "2021-05-26T12:00:00.000Z",
    "NotBefore": "2020-04-26T00:00:00.000Z",
    "Options": {
        "CertificateTransparencyLoggingPreference": "ENABLED",
    }
    "RenewalEligibility": "ELIGIBLE",
    "RenewalSummary": {
        "DomainValidationOptions": [
            {
                "DomainName": "example.amazondomains.com",
                "ResourceRecord": {
                    "Name":
 "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                    "Type": "CNAME",
                    "Value": "_example.acm-validations.aws.com",
                },
                "ValidationDomain": "example.amazondomains.com",
                "ValidationEmails": ["sample_email@sample.com"],
                "ValidationMethod": "DNS",
                "ValidationStatus": "SUCCESS"
            }
        ],
        "RenewalStatus": "SUCCESS",
        "RenewalStatusReason": "",
        "UpdatedAt": "2020-04-26T00:41:35.000Z",
    },
    "Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
    "SignatureAlgorithm": "SHA256WITHRSA",
    "Status": "ISSUED",
    "Subject": "CN=example.amazondomains.com",
    "SubjectAlternativeNames": ["example.amazondomains.com"],
    "Type": "AMAZON_ISSUED"
}
```

AwsCloudFormation

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsCloudFormation` Ressourcen.

AwsCloudFormationStack

Das `AwsCloudFormationStack` Objekt enthält Details zu einem AWS CloudFormation Stapel, der als Ressource in einer Vorlage der obersten Ebene verschachtelt ist.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsCloudFormationStack` Beschreibungen der `AwsCloudFormationStack` Attribute finden Sie AwsCloudFormationStackDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsCloudFormationStack": {
 "Capabilities": [
  "CAPABILITY_IAM",
  "CAPABILITY_NAMED_IAM"
 ],
 "CreationTime": "2022-02-18T15:31:53.161Z",
 "Description": "AWS CloudFormation Sample",
 "DisableRollback": true,
 "DriftInformation": {
  "StackDriftStatus": "DRIFTED"
 },
 "EnableTerminationProtection": false,
 "LastUpdatedTime": "2022-02-18T15:31:53.161Z",
 "NotificationArns": [
  "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
 ],
 "Outputs": [{
  "Description": "URL for newly created LAMP stack",
  "OutputKey": "WebsiteUrl",
  "OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
 }],
 "RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
 "StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/
e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
 "StackName": "sample-stack",
 "StackStatus": "CREATE_COMPLETE",
 "StackStatusReason": "Success",
 "TimeoutInMinutes": 1
}
```

AwsCloudFront

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsCloudFront` Ressourcen.

AwsCloudFrontDistribution

Das `AwsCloudFrontDistribution` Objekt enthält Details zu einer CloudFront Amazon-Vertriebskonfiguration.

Im Folgenden finden Sie ein Beispiel für einen `AwsCloudFrontDistribution` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsCloudFrontDistribution` Attribute finden Sie AwsCloudFrontDistributionDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsCloudFrontDistribution": {
    "CacheBehaviors": {
        "Items": [
            {
               "ViewerProtocolPolicy": "https-only"
            }
         ]
    },
    "DefaultCacheBehavior": {
         "ViewerProtocolPolicy": "https-only"
    },
    "DefaultRootObject": "index.html",
    "DomainName": "d2wkuj2w9l34gt.cloudfront.net",
    "Etag": "E37HOT42DHPVYH",
    "LastModifiedTime": "2015-08-31T21:11:29.093Z",
    "Logging": {
         "Bucket": "myawslogbucket.s3.amazonaws.com",
         "Enabled": false,
         "IncludeCookies": false,
         "Prefix": "myawslog/"
     },
     "OriginGroups": {
          "Items": [
              {
                 "FailoverCriteria": {
                     "StatusCodes": {
                          "Items": [
                              200,
```

```
                            301,
                            404
                        ]
                        "Quantity": 3
                    }
                }
            }
        ]
    },
    "Origins": {
        "Items": [
            {
                "CustomOriginConfig": {
                    "HttpPort": 80,
                    "HttpsPort": 443,
                    "OriginKeepaliveTimeout": 60,
                    "OriginProtocolPolicy": "match-viewer",
                    "OriginReadTimeout": 30,
                    "OriginSslProtocols": {
                      "Items": ["SSLv3", "TLSv1"],
                      "Quantity": 2
                    }
                }
            },
        ]
    },
                "DomainName": "my-bucket.s3.amazonaws.com",
                "Id": "my-origin",
                "OriginPath": "/production",
                "S3OriginConfig": {
                    "OriginAccessIdentity": "origin-access-identity/cloudfront/
E2YFS67H6VB6E4"
                }
        ]
    },
    "Status": "Deployed",
    "ViewerCertificate": {
           "AcmCertificateArn": "arn:aws:acm::123456789012:AcmCertificateArn",
           "Certificate": "ASCAJRRE5XYF52TKRY5M4",
           "CertificateSource": "iam",
           "CloudFrontDefaultCertificate": true,
           "IamCertificateId": "ASCAJRRE5XYF52TKRY5M4",
           "MinimumProtocolVersion": "TLSv1.2_2021",
           "SslSupportMethod": "sni-only"
```

```
      },
      "WebAclId": "waf-1234567890"
}
```

AwsCloudTrail

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsCloudTrail` Ressourcen.

AwsCloudTrailTrail

Das `AwsCloudTrailTrail` Objekt liefert Details zu einer AWS CloudTrail Spur.

Im Folgenden finden Sie ein Beispiel für einen `AwsCloudTrailTrail` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsCloudTrailTrail` Attribute finden Sie AwsCloudTrailTrailDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsCloudTrailTrail": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:CloudTrail/regression:*",
    "CloudWatchLogsRoleArn": "arn:aws:iam::866482105055:role/
CloudTrail_CloudWatchLogs",
    "HasCustomEventSelectors": true,
    "HomeRegion": "us-west-2",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "KmsKeyId": "kmsKeyId",
    "LogFileValidationEnabled": true,
    "Name": "regression-trail",
    "S3BucketName": "cloudtrail-bucket",
    "S3KeyPrefix": "s3KeyPrefix",
    "SnsTopicArn": "arn:aws:sns:us-east-2:123456789012:MyTopic",
    "SnsTopicName": "snsTopicName",
    "TrailArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail"
}
```

AwsCloudWatch

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsCloudWatch` Ressourcen.

AwsCloudWatchAlarm

Das `AwsCloudWatchAlarm` Objekt bietet Details zu CloudWatch Amazon-Alarmen, die eine Metrik beobachten oder eine Aktion ausführen, wenn sich der Status eines Alarms ändert.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsCloudWatchAlarm` Objekt. Beschreibungen der `AwsCloudWatchAlarm` Attribute finden Sie AwsCloudWatchAlarmDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsCloudWatchAlarm": {
 "ActonsEnabled": true,
 "AlarmActions": [
  "arn:aws:automate:region:ec2:stop",
  "arn:aws:automate:region:ec2:terminate"
 ],
 "AlarmArn": "arn:aws:cloudwatch:us-west-2:012345678910:alarm:sampleAlarm",
 "AlarmConfigurationUpdatedTimestamp": "2022-02-18T15:31:53.161Z",
 "AlarmDescription": "Alarm Example",
 "AlarmName": "Example",
 "ComparisonOperator": "GreaterThanOrEqualToThreshold",
 "DatapointsToAlarm": 1,
 "Dimensions": [{
  "Name": "InstanceId",
  "Value": "i-1234567890abcdef0"
 }],
 "EvaluateLowSampleCountPercentile": "evaluate",
 "EvaluationPeriods": 1,
 "ExtendedStatistic": "p99.9",
 "InsufficientDataActions": [
  "arn:aws:automate:region:ec2:stop"
 ],
 "MetricName": "Sample Metric",
 "Namespace": "YourNamespace",
 "OkActions": [
  "arn:aws:swf:region:account-id:action/actions/AWS_EC2.InstanceId.Stop/1.0"
 ],
 "Period": 1,
 "Statistic": "SampleCount",
 "Threshold": 12.3,
 "ThresholdMetricId": "t1",
 "TreatMissingData": "notBreaching",
```

```
 "Unit": "Kilobytes/Second"
}
```

AwsCodeBuild

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsCodeBuild` Ressourcen.

AwsCodeBuildProject

Das Objekt `AwsCodeBuildProject` liefert Informationen zu einem AWS CodeBuild -Projekt.

Im Folgenden finden Sie ein Beispiel für einen `AwsCodeBuildProject` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsCodeBuildProject` Attribute finden Sie AwsCodeBuildProjectDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsCodeBuildProject": {
   "Artifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
   ],
   "SecondaryArtifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
```

```
    ],
    "EncryptionKey": "string",
    "Certificate": "string",
    "Environment": {
       "Certificate": "string",
       "EnvironmentVariables": [
            {
                 "Name": "string",
                 "Type": "string",
                 "Value": "string"
            }
       ],
    "ImagePullCredentialsType": "string",
    "PrivilegedMode": boolean,
    "RegistryCredential": {
        "Credential": "string",
        "CredentialProvider": "string"
    },
    "Type": "string"
    },
    "LogsConfig": {
         "CloudWatchLogs": {
              "GroupName": "string",
              "Status": "string",
              "StreamName": "string"
         },
         "S3Logs": {
              "EncryptionDisabled": boolean,
              "Location": "string",
              "Status": "string"
         }
    },
    "Name": "string",
    "ServiceRole": "string",
    "Source": {
         "Type": "string",
         "Location": "string",
         "GitCloneDepth": integer
    },
    "VpcConfig": {
         "VpcId": "string",
         "Subnets": ["string"],
         "SecurityGroupIds": ["string"]
    }
```

```
}
```

AwsDms

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsDms` Ressourcen.

AwsDmsEndpoint

Das `AwsDmsEndpoint` Objekt stellt Informationen über einen AWS Database Migration Service (AWS DMS) -Endpunkt bereit. Ein Endpunkt stellt Verbindungs-, Datenspeichertyp- und Standortinformationen zu Ihrem Datenspeicher bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsDmsEndpoint` Objekt. Beschreibungen der `AwsDmsEndpoint` Attribute finden Sie AwsDmsEndpointDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsDmsEndpoint": {
    "CertificateArn": "arn:aws:dms:us-
east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWFI",
    "DatabaseName": "Test",
    "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBNPK6MJQVFVQA",
    "EndpointIdentifier": "target-db",
    "EndpointType": "TARGET",
    "EngineName": "mariadb",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "Port": 3306,
    "ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",
    "SslMode": "verify-ca",
    "Username": "admin"
}
```

AwsDmsReplicationInstance

Das `AwsDmsReplicationInstance` Objekt stellt Informationen über eine AWS Database Migration Service (AWS DMS) Replikationsinstanz bereit. DMS verwendet eine Replikationsinstanz, um eine Verbindung zu Ihrem Quelldatenspeicher herzustellen, die Quelldaten zu lesen und die Daten für den Zieldatenspeicher zu formatieren.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsDmsReplicationInstance` Objekt. Beschreibungen der `AwsDmsReplicationInstance` Attribute finden Sie AwsDmsReplicationInstanceDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsDmsReplicationInstance": {
    "AllocatedStorage": 50,
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1b",
    "EngineVersion": "3.5.1",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "MultiAZ": false,
    "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",
    "PubliclyAccessible": true,
    "ReplicationInstanceClass": "dms.c5.xlarge",
    "ReplicationInstanceIdentifier": "second-replication-instance",
    "ReplicationSubnetGroup": {
        "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"
    },
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-003a34e205138138b"
        }
    ]
}
```

AwsDmsReplicationTask

Das `AwsDmsReplicationTask` Objekt stellt Informationen über eine AWS Database Migration Service (AWS DMS) Replikationsaufgabe bereit. Eine Replikationsaufgabe verschiebt einen Datensatz vom Quellendpunkt zum Zielendpunkt.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsDmsReplicationInstance` Objekt. Beschreibungen der `AwsDmsReplicationInstance` Attribute finden Sie AwsDmsReplicationInstancein der AWS Security Hub API-Referenz.

Beispiel

```
"AwsDmsReplicationTask": {
    "CdcStartPosition": "2023-08-28T14:26:22",
```

```
    "Id": "arn:aws:dms:us-
east-1:123456789012:task:YDYUOHZIXWKQSUCBMUCQCNY44SJW74VJNB5DFWQ",
    "MigrationType": "cdc",
    "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4YOUGIMYJUI",
    "ReplicationTaskIdentifier": "test-task",
    "ReplicationTaskSettings": "{\"Logging\":{\"EnableLogging\":false,
\"EnableLogContext\":false,\"LogComponents\":[{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"TRANSFORMATION\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",
\"Id\":\"SOURCE_UNLOAD\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"IO\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TARGET_LOAD\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"PERFORMANCE\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SOURCE_CAPTURE\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SORTER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"REST_SERVER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id
\":\"VALIDATOR_EXT\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"TARGET_APPLY\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TASK_MANAGER
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TABLES_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"METADATA_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_FACTORY\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMON\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"ADDONS\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"DATA_STRUCTURE
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMUNICATION\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_TRANSFER\"}],\"CloudWatchLogGroup
\":null,\"CloudWatchLogStream\":null},\"StreamBufferSettings\":{\"StreamBufferCount
\":3,\"CtrlStreamBufferSizeInMB\":5,\"StreamBufferSizeInMB\":8},\"ErrorBehavior
\":{\"FailOnNoTablesCaptured\":true,\"ApplyErrorUpdatePolicy\":\"LOG_ERROR\",
\"FailOnTransactionConsistencyBreached\":false,\"RecoverableErrorThrottlingMax\":1800,
\"DataErrorEscalationPolicy\":\"SUSPEND_TABLE\",\"ApplyErrorEscalationCount\":0,
\"RecoverableErrorStopRetryAfterThrottlingMax\":true,\"RecoverableErrorThrottling
\":true,\"ApplyErrorFailOnTruncationDdl\":false,\"DataTruncationErrorPolicy\":
\"LOG_ERROR\",\"ApplyErrorInsertPolicy\":\"LOG_ERROR\",\"EventErrorPolicy\":
\"IGNORE\",\"ApplyErrorEscalationPolicy\":\"LOG_ERROR\",\"RecoverableErrorCount
\":-1,\"DataErrorEscalationCount\":0,\"TableErrorEscalationPolicy\":\"STOP_TASK
\",\"RecoverableErrorInterval\":5,\"ApplyErrorDeletePolicy\":\"IGNORE_RECORD\",
\"TableErrorEscalationCount\":0,\"FullLoadIgnoreConflicts\":true,\"DataErrorPolicy
\":\"LOG_ERROR\",\"TableErrorPolicy\":\"SUSPEND_TABLE\"},\"TTSettings
\":{\"TTS3Settings\":null,\"TTRecordSettings\":null,\"EnableTT\":false},
\"FullLoadSettings\":{\"CommitRate\":10000,\"StopTaskCachedChangesApplied
\":false,\"StopTaskCachedChangesNotApplied\":false,\"MaxFullLoadSubTasks
\":8,\"TransactionConsistencyTimeout\":600,\"CreatePkAfterFullLoad\":false,
\"TargetTablePrepMode\":\"DO_NOTHING\"},\"TargetMetadata\":{\"ParallelApplyBufferSize
\":0,\"ParallelApplyQueuesPerThread\":0,\"ParallelApplyThreads\":0,\"TargetSchema
\":\"\",\"InlineLobMaxSize\":0,\"ParallelLoadQueuesPerThread\":0,\"SupportLobs
```

```
\":true,\"LobChunkSize\":64,\"TaskRecoveryTableEnabled\":false,\"ParallelLoadThreads
\":0,\"LobMaxSize\":0,\"BatchApplyEnabled\":false,\"FullLobMode\":true,
\"LimitedSizeLobMode\":false,\"LoadMaxFileSize\":0,\"ParallelLoadBufferSize\":0},
\"BeforeImageSettings\":null,\"ControlTablesSettings\":{\"historyTimeslotInMinutes
\":5,\"HistoryTimeslotInMinutes\":5,\"StatusTableEnabled\":false,
\"SuspendedTablesTableEnabled\":false,\"HistoryTableEnabled\":false,\"ControlSchema
\":\"\",\"FullLoadExceptionTableEnabled\":false},\"LoopbackPreventionSettings
\":null,\"CharacterSetSettings\":null,\"FailTaskWhenCleanTaskResourceFailed
\":false,\"ChangeProcessingTuning\":{\"StatementCacheSize\":50,\"CommitTimeout
\":1,\"BatchApplyPreserveTransaction\":true,\"BatchApplyTimeoutMin\":1,
\"BatchSplitSize\":0,\"BatchApplyTimeoutMax\":30,\"MinTransactionSize\":1000,
\"MemoryKeepTime\":60,\"BatchApplyMemoryLimit\":500,\"MemoryLimitTotal\":1024},
\"ChangeProcessingDdlHandlingPolicy\":{\"HandleSourceTableDropped\":true,
\"HandleSourceTableTruncated\":true,\"HandleSourceTableAltered\":true},
\"PostProcessingRules\":null}",
    "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHYOKVKRNHAKJ4Q3RUXACNGFGYWRI",
    "TableMappings": "{\"rules\":[{\"rule-type\":\"selection\",\"rule-id\":
\"969761702\",\"rule-name\":\"969761702\",\"object-locator\":{\"schema-name\":\"%table
\",\"table-name\":\"%example\"},\"rule-action\":\"exclude\",\"filters\":[]}]}",
    "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:ABR8LBOQB3CZY33F7XV253NAJVBNPK6MJQVFVQA"
}
```


AwsDynamoDB

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsDynamoDB` Ressourcen.

AwsDynamoDbTable

Das `AwsDynamoDbTable` Objekt enthält Details zu einer Amazon DynamoDB-Tabelle.

Im Folgenden finden Sie ein Beispiel für einen `AwsDynamoDbTable` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsDynamoDbTable` Attribute finden Sie AwsDynamoDbTableDetailsin der AWS Security Hub API-Referenz.

Beispiel


```
"AwsDynamoDbTable": {
    "AttributeDefinitions": [
        {
            "AttributeName": "attribute1",
            "AttributeType": "value 1"
```

```
        },
        {
            "AttributeName": "attribute2",
            "AttributeType": "value 2"
        },
        {
            "AttributeName": "attribute3",
            "AttributeType": "value 3"
        }
    ],
    "BillingModeSummary": {
        "BillingMode": "PAY_PER_REQUEST",
        "LastUpdateToPayPerRequestDateTime": "2019-12-03T15:23:10.323Z"
    },
    "CreationDateTime": "2019-12-03T15:23:10.248Z",
    "DeletionProtectionEnabled": true,
    "GlobalSecondaryIndexes": [
        {
            "Backfilling": false,
            "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
index/exampleIndex",
            "IndexName": "standardsControlArnIndex",
            "IndexSizeBytes": 1862513,
            "IndexStatus": "ACTIVE",
            "ItemCount": 20,
            "KeySchema": [
                {
                    "AttributeName": "City",
                    "KeyType": "HASH"
                },
                {
                    "AttributeName": "Date",
                    "KeyType": "RANGE"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
            "ProvisionedThroughput": {
                "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
                "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
                "NumberOfDecreasesToday": 0,
                "ReadCapacityUnits": 100,
```

```
                "WriteCapacityUnits": 50
            },
        }
    ],
    "GlobalTableVersion": "V1",
    "ItemCount": 2705,
    "KeySchema": [
        {
            "AttributeName": "zipcode",
            "KeyType": "HASH"
        }
     ],
     "LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
     "LatestStreamLabel": "2019-12-03T23:23:10.248",
     "LocalSecondaryIndexes": [
        {
            "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",
            "IndexName": "CITY_DATE_INDEX_NAME",
            "KeySchema": [
                {
                    "AttributeName": "zipcode",
                    "KeyType": "HASH"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
        }
    ],
    "ProvisionedThroughput": {
        "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
        "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
        "NumberOfDecreasesToday": 0,
        "ReadCapacityUnits": 100,
        "WriteCapacityUnits": 50
    },
    "Replicas": [
        {
            "GlobalSecondaryIndexes":[
                {
                    "IndexName": "CITY_DATE_INDEX_NAME",
```

```
                    "ProvisionedThroughputOverride": {
                        "ReadCapacityUnits": 10
                    }
                }
            ],
            "KmsMasterKeyId" : "KmsKeyId"
            "ProvisionedThroughputOverride": {
                "ReadCapacityUnits": 10
            },
            "RegionName": "regionName",
            "ReplicaStatus": "CREATING",
            "ReplicaStatusDescription": "replicaStatusDescription"
        }
    ],
    "RestoreSummary" : {
        "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
backup/backup1",
        "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
        "RestoreDateTime": "2020-06-22T17:40:12.322Z",
        "RestoreInProgress": true
    },
    "SseDescription": {
        "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
        "Status": "ENABLED",
        "SseType": "KMS",
        "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
    },
    "StreamSpecification" : {
        "StreamEnabled": true,
        "StreamViewType": "NEW_IMAGE"
    },
    "TableId": "example-table-id-1",
    "TableName": "example-table",
    "TableSizeBytes": 1862513,
    "TableStatus": "ACTIVE"
}
```

AwsEc2

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsEc2` Ressourcen.

AwsEc2ClientVpnEndpoint

Das `AwsEc2ClientVpnEndpoint` Objekt stellt Informationen über einen AWS Client VPN Endpunkt bereit. Ein Client-VPN-Endpunkt ist die Ressource, die Sie erstellen und konfigurieren, um Client-VPN-Sitzungen zu aktivieren und zu verwalten. Es handelt sich hier um den Beendigungspunkt für alle Client-VPN-Sitzungen.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2ClientVpnEndpoint` Objekt. Beschreibungen der `AwsEc2ClientVpnEndpoint` Attribute finden Sie unter AwsEc2 ClientVpnEndpointDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2ClientVpnEndpoint": {
    "AuthenticationOptions": [
        {
            "MutualAuthentication": {
                "ClientRootCertificateChainArn": "arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
            "Type": "certificate-authentication"
        }
    ],
    "ClientCidrBlock": "10.0.0.0/22",
    "ClientConnectOptions": {
        "Enabled": false
    },
    "ClientLoginBannerOptions": {
        "Enabled": false
    },
    "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
    "ConnectionLogOptions": {
        "Enabled": false
    },
    "Description": "test",
    "DnsServer": ["10.0.0.0"],
    "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "SecurityGroupIdSet": [
        "sg-0f7a177b82b443691"
    ],
    "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/
cvpn-endpoint-00c5d11fc4729f2a5",
```

```
    "SessionTimeoutHours": 24,
    "SplitTunnel": false,
    "TransportProtocol": "udp",
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
    "VpnPort": 443
}
```

AwsEc2Eip

Das `AwsEc2Eip` Objekt stellt Informationen über eine Elastic IP-Adresse bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2Eip` Objekt. Beschreibungen der `AwsEc2Eip` Attribute finden Sie unter AwsEc2 EipDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2Eip": {
    "InstanceId": "instance1",
    "PublicIp": "192.0.2.04",
    "AllocationId": "eipalloc-example-id-1",
    "AssociationId": "eipassoc-example-id-1",
    "Domain": "vpc",
    "PublicIpv4Pool": "anycompany",
    "NetworkBorderGroup": "eu-central-1",
    "NetworkInterfaceId": "eni-example-id-1",
    "NetworkInterfaceOwnerId": "777788889999",
    "PrivateIpAddress": "192.0.2.03"
}
```

AwsEc2Instance

Das `AwsEc2Instance` Objekt enthält Details zu einer Amazon EC2 EC2-Instance.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2Instance` Objekt. Beschreibungen der `AwsEc2Instance` Attribute finden Sie unter AwsEc2 InstanceDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
```

```
    "ImageId": "ami-1234",
    "IpV4Addresses": [ "1.1.1.1" ],
    "IpV6Addresses": [ "2001:db8:1234:1a2b::123" ],
    "KeyName": "my_keypair",
    "LaunchedAt": "2018-05-08T16:46:19.000Z",
    "MetadataOptions": {
     "HttpEndpoint": "enabled",
     "HttpProtocolIpv6": "enabled",
     "HttpPutResponseHopLimit": 1,
     "HttpTokens": "optional",
     "InstanceMetadataTags": "disabled",
    },
    "Monitoring": {
     "State": "disabled"
    },
    "NetworkInterfaces": [
      {
         "NetworkInterfaceId": "eni-e5aa89a3"
      }
    ],
    "SubnetId": "subnet-123",
    "Type": "i3.xlarge",
    "VpcId": "vpc-123"
}
```

AwsEc2LaunchTemplate

Das `AwsEc2LaunchTemplate` Objekt enthält Details zu einer Amazon Elastic Compute Cloud-Startvorlage, die Informationen zur Instance-Konfiguration spezifiziert.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2LaunchTemplate` Objekt. Beschreibungen der `AwsEc2LaunchTemplate` Attribute finden Sie unter AwsEc2 LaunchTemplateDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "1",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "lt-0a16e9802800bdd85",
    "ImageId": "ami-0d5eff06f840b45e9",
    "LatestVersionNumber": "1",
```

```
    "LaunchTemplateData": {
     "BlockDeviceMappings": [{
      "DeviceName": "/dev/xvda",
      "Ebs": {
       "DeleteonTermination": true,
       "Encrypted": true,
       "SnapshotId": "snap-01047646ec075f543",
       "VolumeSize": 8,
       "VolumeType:" "gp2"
      }
     }],
     "MetadataOptions": {
      "HttpTokens": "enabled",
      "HttpPutResponseHopLimit" : 1
     },
     "Monitoring": {
      "Enabled": true,
     "NetworkInterfaces": [{
      "AssociatePublicIpAddress" : true,
     }],
    "LaunchTemplateName": "string",
    "LicenseSpecifications": ["string"],
    "SecurityGroupIds": ["sg-01fce87ad6e019725"],
    "SecurityGroups": ["string"],
    "TagSpecifications": ["string"]
}
```

AwsEc2NetworkAcl

Das `AwsEc2NetworkAcl` Objekt enthält Details zu einer Amazon EC2 EC2-Netzwerkzugriffskontrollliste (ACL).

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2NetworkAcl` Objekt. Beschreibungen der `AwsEc2NetworkAcl` Attribute finden Sie unter AwsEc2 NetworkAclDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2NetworkAcl": {
    "IsDefault": false,
    "NetworkAclId": "acl-1234567890abcdef0",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234abcd",
```

```
    "Associations": [{
        "NetworkAclAssociationId": "aclassoc-abcd1234",
        "NetworkAclId": "acl-021345abcdef6789",
        "SubnetId": "subnet-abcd1234"
   }],
   "Entries": [{
        "CidrBlock": "10.24.34.0/23",
        "Egress": true,
        "IcmpTypeCode": {
            "Code": 10,
            "Type": 30
        },
        "Ipv6CidrBlock": "2001:DB8::/32",
        "PortRange": {
            "From": 20,
            "To": 40
        },
        "Protocol": "tcp",
        "RuleAction": "allow",
        "RuleNumber": 100
   }]
}
```

AwsEc2NetworkInterface

Das `AwsEc2NetworkInterface` Objekt stellt Informationen über eine Amazon EC2 EC2-Netzwerkschnittstelle bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2NetworkInterface` Objekt. Beschreibungen der `AwsEc2NetworkInterface` Attribute finden Sie unter AwsEc2 NetworkInterfaceDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2NetworkInterface": {
    "Attachment": {
        "AttachTime": "2019-01-01T03:03:21Z",
        "AttachmentId": "eni-attach-43348162",
        "DeleteOnTermination": true,
        "DeviceIndex": 123,
        "InstanceId": "i-1234567890abcdef0",
        "InstanceOwnerId": "123456789012",
        "Status": 'ATTACHED'
```

```
    },
    "SecurityGroups": [
        {
            "GroupName": "my-security-group",
            "GroupId": "sg-903004f8"
        },
    ],
    "NetworkInterfaceId": 'eni-686ea200',
    "SourceDestCheck": false
}
```

AwsEc2RouteTable

Das `AwsEc2RouteTable` Objekt stellt Informationen über eine Amazon EC2 EC2-Routentabelle bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2RouteTable` Objekt. Beschreibungen der `AwsEc2RouteTable` Attribute finden Sie unter AwsEc2 RouteTableDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2RouteTable": {
    "AssociationSet": [{
     "AssociationSet": {
      "State": "associated"
        },
     "Main": true,
     "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
     "RouteTableId": "rtb-0a59bde9cf2548e34",
    }],
    "PropogatingVgwSet": [],
    "RouteTableId": "rtb-0a59bde9cf2548e34",
    "RouteSet": [
     {
      "DestinationCidrBlock": "10.24.34.0/23",
      "GatewayId": "local",
      "Origin": "CreateRouteTable",
      "State": "active"
     },
     {
      "DestinationCidrBlock": "10.24.34.0/24",
      "GatewayId": "igw-0242c2d7d513fc5d3",
```

```
      "Origin": "CreateRoute",
      "State": "active"
     }
    ],
    "VpcId": "vpc-0c250a5c33f51d456"
}
```

AwsEc2SecurityGroup

Das `AwsEc2SecurityGroup` Objekt beschreibt eine Amazon EC2-Sicherheitsgruppe.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2SecurityGroup` Objekt. Beschreibungen der `AwsEc2SecurityGroup` Attribute finden Sie unter AwsEc2 SecurityGroupDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2SecurityGroup": {
    "GroupName": "MySecurityGroup",
    "GroupId": "sg-903004f8",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1a2b3c4d",
    "IpPermissions": [
        {
            "IpProtocol": "-1",
            "IpRanges": [],
            "UserIdGroupPairs": [
                {
                    "UserId": "123456789012",
                    "GroupId": "sg-903004f8"
                }
            ],
            "PrefixListIds": [
                {"PrefixListId": "pl-63a5400a"}
            ]
        },
        {
            "PrefixListIds": [],
            "FromPort": 22,
            "IpRanges": [
                {
                    "CidrIp": "203.0.113.0/24"
                }
```

```
            ],
            "ToPort": 22,
            "IpProtocol": "tcp",
            "UserIdGroupPairs": []
        }
    ]
}
```

AwsEc2Subnet

Das `AwsEc2Subnet` Objekt stellt Informationen über ein Subnetz in Amazon EC2 bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsEc2Subnet` Beschreibungen der `AwsEc2Subnet` Attribute finden Sie unter AwsEc2 SubnetDetails in der AWS Security Hub API-Referenz.

Beispiel

```
AwsEc2Subnet: {
    "AssignIpv6AddressOnCreation": false,
    "AvailabilityZone": "us-west-2c",
    "AvailabilityZoneId": "usw2-az3",
    "AvailableIpAddressCount": 8185,
    "CidrBlock": "10.0.0.0/24",
    "DefaultForAz": false,
    "MapPublicIpOnLaunch": false,
    "OwnerId": "123456789012",
    "State": "available",
    "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/subnet-d5436c93",
    "SubnetId": "subnet-d5436c93",
    "VpcId": "vpc-153ade70",
    "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "subnet-cidr-assoc-EXAMPLE",
        "Ipv6CidrBlock": "2001:DB8::/32",
        "CidrBlockState": "associated"
   }]
}
```

AwsEc2TransitGateway

Das `AwsEc2TransitGateway` Objekt enthält Details zu einem Amazon EC2-Transit-Gateway, das Ihre virtuellen privaten Clouds (VPCs) und lokalen Netzwerke miteinander verbindet.

Im Folgenden finden Sie ein Beispiel für einen `AwsEc2TransitGateway` Befund im AWS Security Finding Format (ASFF). Beschreibungen von `AwsEc2TransitGateway` Attributen finden Sie unter AwsEc2 TransitGatewayDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2TransitGateway": {
 "AmazonSideAsn": 65000,
 "AssociationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "AutoAcceptSharedAttachments": "disable",
 "DefaultRouteTableAssociation": "enable",
 "DefaultRouteTablePropagation": "enable",
 "Description": "sample transit gateway",
 "DnsSupport": "enable",
 "Id": "tgw-042ae6bf7a5c126c3",
 "MulticastSupport": "disable",
 "PropagationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "TransitGatewayCidrBlocks": ["10.0.0.0/16"],
 "VpnEcmpSupport": "enable"
}
```

AwsEc2Volume

Das `AwsEc2Volume` Objekt enthält Details zu einem Amazon EC2 EC2-Volume.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2Volume` Objekt. Beschreibungen der `AwsEc2Volume` Attribute finden Sie unter AwsEc2 VolumeDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2Volume": {
    "Attachments": [
      {
        "AttachTime": "2017-10-17T14:47:11Z",
        "DeleteOnTermination": true,
        "InstanceId": "i-123abc456def789g",
        "Status": "attached"
      }
     ],
    "CreateTime": "2020-02-24T15:54:30Z",
    "Encrypted": true,
```

```
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "Size": 80,
    "SnapshotId": "",
    "Status": "available"
}
```

AwsEc2Vpc

Das `AwsEc2Vpc` Objekt enthält Details zu einer Amazon EC2 EC2-VPC.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsEc2Vpc` Beschreibungen der `AwsEc2Vpc` Attribute finden Sie unter AwsEc2 VpcDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2Vpc": {
    "CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlock": "192.0.2.0/24",
            "CidrBlockState": "associated"
        }
    ],
    "DhcpOptionsId": "dopt-4e42ce28",
    "Ipv6CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlockState": "associated",
            "Ipv6CidrBlock": "192.0.2.0/24"
       }

    ],
    "State": "available"
}
```

AwsEc2VpcEndpointService

Das `AwsEc2VpcEndpointService` Objekt enthält Details zur Dienstkonfiguration für einen VPC-Endpunktdienst.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2VpcEndpointService` Objekt. Beschreibungen der `AwsEc2VpcEndpointService` Attribute finden Sie unter AwsEc2 VpcEndpointServiceDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2VpcEndpointService": {
    "ServiceType": [
      {
        "ServiceType": "Interface"
      }
    ],
    "ServiceId": "vpce-svc-example1",
    "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example1",
    "ServiceState": "Available",
    "AvailabilityZones": [
      "us-east-1"
    ],
    "AcceptanceRequired": true,
    "ManagesVpcEndpoints": false,
    "NetworkLoadBalancerArns": [
      "arn:aws:elasticloadbalancing:us-east-1:444455556666:loadbalancer/net/my-network-
load-balancer/example1"
    ],
    "GatewayLoadBalancerArns": [],
    "BaseEndpointDnsNames": [
      "vpce-svc-04eec859668b51c34.us-east-1.vpce.amazonaws.com"
    ],
    "PrivateDnsName": "my-private-dns"
}
```

AwsEc2VpcPeeringConnection

Das `AwsEc2VpcPeeringConnection` Objekt enthält Details zur Netzwerkverbindung zwischen zwei VPCs.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2VpcPeeringConnection` Objekt. Beschreibungen der `AwsEc2VpcPeeringConnection` Attribute finden Sie unter AwsEc2 VpcPeeringConnectionDetails in der AWS Security Hub API-Referenz.

Beispiel


```
"AwsEc2VpcPeeringConnection": {
 "AccepterVpcInfo": {
  "CidrBlock": "10.0.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "10.0.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "ExpirationTime": "2022-02-18T15:31:53.161Z",
 "RequesterVpcInfo": {
  "CidrBlock": "192.168.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "192.168.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "Status": {
  "Code": "initiating-request",
  "Message": "Active"
 },
 "VpcPeeringConnectionId": "pcx-1a2b3c4d"
```

```
}
```

AwsEc2VpnConnection

Das `AwsEc2VpnConnection` Objekt bietet Details zu einer Amazon EC2 EC2-VPN-Verbindung.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEc2VpnConnection` Objekt. Beschreibungen der `AwsEc2VpnConnection` Attribute finden Sie unter AwsEc2 VpnConnectionDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEc2VpnConnection": {
    "VpnConnectionId": "vpn-205e4f41",
    "State": "available",
    "CustomerGatewayConfiguration": "",
    "CustomerGatewayId": "cgw-5699703f",
    "Type": "ipsec.1",
    "VpnGatewayId": "vgw-2ccb2245",
    "Category": "VPN"
    "TransitGatewayId": "tgw-09b6f3a659e2b5elf",
    "VgwTelemetry": [
        {
            "OutsideIpAddress": "92.0.2.11",
            "Status": "DOWN",
            "LastStatusChange": "2016-11-11T23:09:32.000Z",
            "StatusMessage": "IPSEC IS DOWN",
            "AcceptedRouteCount": 0
        },
        {
            "OutsideIpAddress": "92.0.2.12",
            "Status": "DOWN",
            "LastStatusChange": "2016-11-11T23:10:51.000Z",
            "StatusMessage": "IPSEC IS DOWN",
            "AcceptedRouteCount": 0
        }
    ],
    "Routes": [{
        "DestinationCidrBlock": "10.24.34.0/24",
        "State": "available"
   }],
    "Options": {
        "StaticRoutesOnly": true
```

```
        "TunnelOptions": [{
            "DpdTimeoutSeconds": 30,
            "IkeVersions": ["ikev1", "ikev2"],
            "Phase1DhGroupNumbers": [14, 15, 16, 17, 18},
            "Phase1EncryptionAlgorithms": ["AES128", "AES256"],
            "Phase1IntegrityAlgorithms": ["SHA1", "SHA2-256"],
            "Phase1LifetimeSeconds": 28800,
            "Phase2DhGroupNumbers": [14, 15, 16, 17, 18],
            "Phase2EncryptionAlgorithms": ["AES128", "AES256"],
            "Phase2IntegrityAlgorithms": ["SHA1", "SHA2-256"],
            "Phase2LifetimeSeconds": 28800,
            "PreSharedKey": "RltXC3REhTw1RAdiM2s1uMfkkSDLyGJoe1QEWeGxqkQ=",
            "RekeyFuzzPercentage": 100,
            "RekeyMarginTimeSeconds": 540,
            "ReplayWindowSize": 1024,
            "TunnelInsideCidr": "10.24.34.0/23"
        }]
    }
}
```

AwsEcr

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsEcr` Ressourcen.

AwsEcrContainerImage

Das `AwsEcrContainerImage` Objekt stellt Informationen zu einem Amazon ECR-Bild bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcrContainerImage` Objekt. Beschreibungen der `AwsEcrContainerImage` Attribute finden Sie AwsEcrContainerImageDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEcrContainerImage": {
    "RegistryId": "123456789012",
    "RepositoryName": "repository-name",
    "Architecture": "amd64"
    "ImageDigest":
 "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
    "ImageTags": ["00000000-0000-0000-0000-000000000000"],
    "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

Das `AwsEcrRepository` Objekt stellt Informationen über ein Amazon Elastic Container Registry-Repository bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcrRepository` Objekt. Beschreibungen der `AwsEcrRepository` Attribute finden Sie AwsEcrRepositoryDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEcrRepository": {
    "LifecyclePolicy": {
        "RegistryId": "123456789012",
    },
    "RepositoryName": "sample-repo",
    "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
    "ImageScanningConfiguration": {
        "ScanOnPush": true
    },
    "ImageTagMutability": "IMMUTABLE"
}
```

AwsEcs

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsEcs` Ressourcen.

AwsEcsCluster

Das `AwsEcsCluster` Objekt enthält Details zu einem Amazon Elastic Container Service-Cluster.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcsCluster` Objekt. Beschreibungen der `AwsEcsCluster` Attribute finden Sie AwsEcsClusterDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
    "AwsEcsCluster": {
        "CapacityProviders": [],
        "ClusterSettings": [
            {
                "Name": "containerInsights",
                "Value": "enabled"
```

```
            }
        ],
        "Configuration": {
            "ExecuteCommandConfiguration": {
                "KmsKeyId": "kmsKeyId",
                "LogConfiguration": {
                    "CloudWatchEncryptionEnabled": true,
                    "CloudWatchLogGroupName": "cloudWatchLogGroupName",
                    "S3BucketName": "s3BucketName",
                    "S3EncryptionEnabled": true,
                    "S3KeyPrefix": "s3KeyPrefix"
                },
                "Logging": "DEFAULT"
            }
        }
        "DefaultCapacityProviderStrategy": [
            {
                "Base": 0,
                "CapacityProvider": "capacityProvider",
                "Weight": 1
            }
        ]
    }
```

AwsEcsContainer

Das `AwsEcsContainer` Objekt enthält Details zu einem Amazon ECS-Container.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcsContainer` Objekt. Beschreibungen der `AwsEcsContainer` Attribute finden Sie AwsEcsContainerDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEcsContainer": {
    "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
        "ContainerPath": "/mnt/etc",
        "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
```

```
}
```

AwsEcsService

Das `AwsEcsService` Objekt bietet Details zu einem Service innerhalb eines Amazon ECS-Clusters.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcsService` Objekt. Beschreibungen der `AwsEcsService` Attribute finden Sie AwsEcsServiceDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEcsService": {
    "CapacityProviderStrategy": [
        {
            "Base": 12,
            "CapacityProvider": "",
            "Weight": ""
        }
    ],
    "Cluster": "arn:aws:ecs:us-east-1:111122223333:cluster/example-ecs-cluster",
    "DeploymentConfiguration": {
        "DeploymentCircuitBreaker": {
            "Enable": false,
            "Rollback": false
        },
        "MaximumPercent": 200,
        "MinimumHealthyPercent": 100
    },
    "DeploymentController": "",
    "DesiredCount": 1,
    "EnableEcsManagedTags": false,
    "EnableExecuteCommand": false,
    "HealthCheckGracePeriodSeconds": 1,
    "LaunchType": "FARGATE",
    "LoadBalancers": [
        {
            "ContainerName": "",
            "ContainerPort": 23,
            "LoadBalancerName": "",
            "TargetGroupArn": ""
        }
    ],
```

```
    "Name": "sample-app-service",
    "NetworkConfiguration": {
        "AwsVpcConfiguration": {
            "Subnets": [
                "Subnet-example1",
                "Subnet-example2"
            ],
        "SecurityGroups": [
                "Sg-0ce48e9a6e5b457f5"
        ],
        "AssignPublicIp": "ENABLED"
        }
    },
    "PlacementConstraints": [
        {
            "Expression": "",
            "Type": ""
        }
    ],
    "PlacementStrategies": [
        {
            "Field": "",
            "Type": ""
        }
    ],
    "PlatformVersion": "LATEST",
    "PropagateTags": "",
    "Role": "arn:aws:iam::111122223333:role/aws-servicerole/ecs.amazonaws.com/
ServiceRoleForECS",
    "SchedulingStrategy": "REPLICA",
    "ServiceName": "sample-app-service",
    "ServiceArn": "arn:aws:ecs:us-east-1:111122223333:service/example-ecs-cluster/
sample-app-service",
    "ServiceRegistries": [
        {
            "ContainerName": "",
            "ContainerPort": 1212,
            "Port": 1221,
            "RegistryArn": ""
        }
    ],
    "TaskDefinition": "arn:aws:ecs:us-east-1:111122223333:task-definition/example-
taskdef:1"
```

```
}
```

AwsEcsTask

Das `AwsEcsTask` Objekt enthält Details zu einer Amazon ECS-Aufgabe.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcsTask` Objekt. Beschreibungen der `AwsEcsTask` Attribute finden Sie AwsEcsTaskin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEcsTask": {
 "ClusterArn": "arn:aws:ecs:us-west-2:123456789012:task/MyCluster/1234567890123456789",
 "CreatedAt": "1557134011644",
 "Group": "service:fargate-service",
 "StartedAt": "1557134011644",
 "StartedBy": "ecs-svc/1234567890123456789",
 "TaskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/sample-
fargate:2",
 "Version": 3,
 "Volumes": [{
  "Name": "string",
  "Host": {
   "SourcePath": "string"
  }
 }],
 "Containers": {
  "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
   "ContainerPath": "/mnt/etc",
   "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
 }
}
```

AwsEcsTaskDefinition

Das `AwsEcsTaskDefinition` Objekt enthält Details zu einer Aufgabendefinition. Eine Aufgabendefinition beschreibt die Container- und Volume-Definitionen einer Amazon Elastic Container Service-Aufgabe.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEcsTaskDefinition` Objekt. Beschreibungen der `AwsEcsTaskDefinition` Attribute finden Sie AwsEcsTaskDefinitionDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
    "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [
            {
                "Command": ['ruby', 'hi.rb'],
                "Cpu":128,
                "Essential": true,
                "HealthCheck": {
                    "Command": ["CMD-SHELL", "curl -f http://localhost/ || exit 1"],
                    "Interval": 10,
                    "Retries": 3,
                    "StartPeriod": 5,
                    "Timeout": 20
                },
                "Image": "tongueroo/sinatra:latest",
                "Interactive": true,
                "Links": [],
                "LogConfiguration": {
                    "LogDriver": "awslogs",
                    "Options": {
                        "awslogs-group": "/ecs/sinatra-hi",
                        "awslogs-region": "ap-southeast-1",
                        "awslogs-stream-prefix": "ecs"
                    },
                    "SecretOptions": []

                },
                "MemoryReservation": 128,
                "Name": "web",
                "PortMappings": [
                    {
                        "ContainerPort": 4567,
```

```
                    "HostPort":4567,
                    "Protocol": "tcp"
                }
            ],
            "Privileged": true,
            "StartTimeout": 10,
            "StopTimeout": 100,
        }
    ],
    "Family": "sinatra-hi",
    "NetworkMode": "host",
    "RequiresCompatibilities": ["EC2"],
    "Status": "ACTIVE",
    "TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
}
```

AwsEfs

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsEfs` Ressourcen.

AwsEfsAccessPoint

Das `AwsEfsAccessPoint` Objekt enthält Details zu Dateien, die im Amazon Elastic File System gespeichert sind.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEfsAccessPoint` Objekt. Beschreibungen der `AwsEfsAccessPoint` Attribute finden Sie AwsEfsAccessPointDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEfsAccessPoint": {
 "AccessPointId": "fsap-05c4c0e79ba0b118a",
 "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/
fsap-05c4c0e79ba0b118a",
 "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
 "FileSystemId": "fs-0f8137f731cb32146",
 "PosixUser": {
  "Gid": "1000",
  "SecondaryGids": ["0", "4294967295"],
  "Uid": "1234"
 },
 "RootDirectory": {
  "CreationInfo": {
```

```
    "OwnerGid": "1000",
    "OwnerUid": "1234",
    "Permissions": "777"
   },
   "Path": "/tmp/example"
  }
}
```

AwsEks

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsEks` Ressourcen.

AwsEksCluster

Das `AwsEksCluster` Objekt enthält Details zu einem Amazon EKS-Cluster.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsEksCluster` Objekt. Beschreibungen der `AwsEksCluster` Attribute finden Sie AwsEksClusterDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
{
  "AwsEksCluster": {
    "Name": "example",
    "Arn": "arn:aws:eks:us-west-2:222222222222:cluster/example",
    "CreatedAt": 1565804921.901,
    "Version": "1.12",
    "RoleArn": "arn:aws:iam::222222222222:role/example-cluster-
ServiceRole-1XWBQWYSFRE2Q",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": false,
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
    "Logging": {
      "ClusterLogging": [
        {
```

```
          "Types": [
            "api",
            "audit",
            "authenticator",
            "controllerManager",
            "scheduler"
          ],
          "Enabled": true
        }
      ]
    },
    "Status": "CREATING",
    "CertificateAuthorityData": {},
  }
}
```

AwsElasticBeanstalk

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsElasticBeanstalk` Ressourcen.

AwsElasticBeanstalkEnvironment

Das `AwsElasticBeanstalkEnvironment` Objekt enthält Details zu einer AWS Elastic Beanstalk Umgebung.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsElasticBeanstalkEnvironment` Objekt. Beschreibungen der `AwsElasticBeanstalkEnvironment` Attribute finden Sie AwsElasticBeanstalkEnvironmentDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsElasticBeanstalkEnvironment": {
    "ApplicationName": "MyApplication",
    "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
    "DateCreated": "2021-04-30T01:38:01.090Z",
    "DateUpdated": "2021-04-30T01:38:01.090Z",
    "Description": "Example description of my awesome application",
    "EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-
east-1.elb.amazonaws.com",
    "EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/
MyApplication/myapplication-env",
```

```
    "EnvironmentId": "e-abcd1234",
    "EnvironmentLinks": [
        {
            "EnvironmentName": "myexampleapp-env",
            "LinkName": "myapplicationLink"
        }
    ],
    "EnvironmentName": "myapplication-env",
    "OptionSettings": [
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSize",
            "Value": "100"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "Timeout",
            "Value": "600"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSizeType",
            "Value": "Percentage"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "IgnoreHealthCheck",
            "Value": "false"
        },
        {
            "Namespace": "aws:elasticbeanstalk:application",
            "OptionName": "Application Healthcheck URL",
            "Value": "TCP:80"
        }
    ],
    "PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
running on 64bit Amazon Linux/2.7.7",
    "SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
    "Status": "Ready",
    "Tier": {
        "Name": "WebServer"
       "Type": "Standard"
       "Version": "1.0"
    },
```

```
    "VersionLabel": "Sample Application"
}
```

AwsElasticSearch

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsElasticSearch` Ressourcen.

AwsElasticSearchDomain

Das `AwsElasticSearchDomain` Objekt enthält Details zu einer Amazon OpenSearch Service-Domain.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsElasticSearchDomain` Objekt. Beschreibungen der `AwsElasticSearchDomain` Attribute finden Sie AwsElasticSearchDomainDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsElasticSearchDomain": {
    "AccessPolicies": "string",
    "DomainStatus": {
           "DomainId": "string",
           "DomainName": "string",
           "Endpoint": "string",
           "Endpoints": {
                  "string": "string"
           }
    },
    "DomainEndpointOptions": {
           "EnforceHTTPS": boolean,
           "TLSSecurityPolicy": "string"
    },
    "ElasticsearchClusterConfig": {
           "DedicatedMasterCount": number,
           "DedicatedMasterEnabled": boolean,
           "DedicatedMasterType": "string",
           "InstanceCount": number,
           "InstanceType": "string",
           "ZoneAwarenessConfig": {
                  "AvailabilityZoneCount": number
           },
           "ZoneAwarenessEnabled": boolean
```

```
    },
    "ElasticsearchVersion": "string",
    "EncryptionAtRestOptions": {
           "Enabled": boolean,
           "KmsKeyId": "string"
    },
    "LogPublishingOptions": {
           "AuditLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
           },
           "IndexSlowLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
           },
           "SearchSlowLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
           }
    },
    "NodeToNodeEncryptionOptions": {
           "Enabled": boolean
    },
    "ServiceSoftwareOptions": {
           "AutomatedUpdateDate": "string",
           "Cancellable": boolean,
           "CurrentVersion": "string",
           "Description": "string",
           "NewVersion": "string",
           "UpdateAvailable": boolean,
           "UpdateStatus": "string"
    },
    "VPCOptions": {
           "AvailabilityZones": [
                 "string"
           ],
           "SecurityGroupIds": [
                 "string"
           ],
           "SubnetIds": [
                 "string"
           ],
          "VPCId": "string"
    }
```

```
}
```

AwsElb

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsElb` Ressourcen.

AwsElbLoadBalancer

Das `AwsElbLoadBalancer` Objekt enthält Details zu einem Classic Load Balancer.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsElbLoadBalancer` Objekt. Beschreibungen der `AwsElbLoadBalancer` Attribute finden Sie AwsElbLoadBalancerDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsElbLoadBalancer": {
    "AvailabilityZones": ["us-west-2a"],
    "BackendServerDescriptions": [
         {
            "InstancePort": 80,
            "PolicyNames": ["doc-example-policy"]
        }
    ],
    "CanonicalHostedZoneName": "Z3DZXE0EXAMPLE",
    "CanonicalHostedZoneNameID": "my-load-balancer-444455556666.us-
west-2.elb.amazonaws.com",
    "CreatedTime": "2020-08-03T19:22:44.637Z",
    "DnsName": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
    "HealthCheck": {
        "HealthyThreshold": 2,
        "Interval": 30,
        "Target": "HTTP:80/png",
        "Timeout": 3,
        "UnhealthyThreshold": 2
    },
    "Instances": [
        {
            "InstanceId": "i-example"
        }
    ],
    "ListenerDescriptions": [
        {
            "Listener": {
```

```
                "InstancePort": 443,
                "InstanceProtocol": "HTTPS",
                "LoadBalancerPort": 443,
                "Protocol": "HTTPS",
                "SslCertificateId": "arn:aws:iam::444455556666:server-certificate/my-
server-cert"
            },
            "PolicyNames": ["ELBSecurityPolicy-TLS-1-2-2017-01"]
        }
    ],
    "LoadBalancerAttributes": {
        "AccessLog": {
            "EmitInterval": 60,
            "Enabled": true,
            "S3BucketName": "doc-example-bucket",
            "S3BucketPrefix": "doc-example-prefix"
        },
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        },
        "ConnectionSettings": {
            "IdleTimeout": 30
        },
        "CrossZoneLoadBalancing": {
            "Enabled": true
        },
        "AdditionalAttributes": [{
            "Key": "elb.http.desyncmitigationmode",
            "Value": "strictest"
        }]

    },
    "LoadBalancerName": "example-load-balancer",
    "Policies": {
        "AppCookieStickinessPolicies": [
            {
                "CookieName": "",
                "PolicyName": ""
            }
        ],
        "LbCookieStickinessPolicies": [
            {
                "CookieExpirationPeriod": 60,
```

```
                "PolicyName": "my-example-cookie-policy"
            }
        ],
        "OtherPolicies": [
            "my-PublicKey-policy",
            "my-authentication-policy",
            "my-SSLNegotiation-policy",
            "my-ProxyProtocol-policy",
            "ELBSecurityPolicy-2015-03"
        ]
    },
    "Scheme": "internet-facing",
    "SecurityGroups": ["sg-example"],
    "SourceSecurityGroup": {
        "GroupName": "my-elb-example-group",
        "OwnerAlias": "444455556666"
    },
    "Subnets": ["subnet-example"],
    "VpcId": "vpc-a01106c2"
}
```

AwsElbv2LoadBalancer

Das Objekt `AwsElbv2LoadBalancer` stellt Informationen über einen Load Balancer bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsElbv2LoadBalancer` Objekt. Beschreibungen der `AwsElbv2LoadBalancer` Attribute finden Sie unter AwsElbv2 LoadBalancerDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsElbv2LoadBalancer": {
                        "AvailabilityZones": {
                            "SubnetId": "string",
                            "ZoneName": "string"
                        },
                        "CanonicalHostedZoneId": "string",
                        "CreatedTime": "string",
                        "DNSName": "string",
                        "IpAddressType": "string",
                        "LoadBalancerAttributes": [
                            {
                                "Key": "string",
```

```
                        "Value": "string"
                    }
                ],
                "Scheme": "string",
                "SecurityGroups": [ "string" ],
                "State": {
                    "Code": "string",
                    "Reason": "string"
                },
                "Type": "string",
                "VpcId": "string"
            }
```

AwsEventBridge

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsEventBridge` Ressourcen.

AwsEventSchemasRegistry

Das `AwsEventSchemasRegistry` Objekt stellt Informationen über eine EventBridge Amazon-Schemaregistrierung bereit. Ein Schema definiert die Struktur der Ereignisse, an die gesendet werden EventBridge. Schemaregister sind Container, die Ihre Schemas sammeln und logisch gruppieren.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsEventSchemasRegistry` Beschreibungen der `AwsEventSchemasRegistry` Attribute finden Sie AwsEventSchemasRegistryin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}
```

AwsEventsEndpoint

Das `AwsEventsEndpoint` Objekt stellt Informationen über einen EventBridge globalen Amazon-Endpunkt bereit. Der Endpunkt kann die Verfügbarkeit Ihrer Anwendung verbessern, indem er sie regional fehlertolerant macht.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsEventsEndpoint` Beschreibungen der `AwsEventsEndpoint` Attribute finden Sie AwsEventsEndpointDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEventsEndpoint": {
    "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
    "Description": "This is a sample endpoint.",
    "EndpointId": "04k1exajoy.veo",
    "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
    "EventBuses": [
        {
            "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
        },
        {
            "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
        }
    ],
    "Name": "my-endpoint",
    "ReplicationConfig": {
        "State": "ENABLED"
    },
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/
Amazon_EventBridge_Invoke_Event_Bus_1258925394",
    "RoutingConfig": {
        "FailoverConfig": {
            "Primary": {
                "HealthCheck": "arn:aws:route53:::healthcheck/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
            },
            "Secondary": {
                "Route": "us-east-2"
            }
        }
    },
    "State": "ACTIVE"
}
```

AwsEventsEventbus

Das `AwsEventsEventbus` Objekt stellt Informationen über einen EventBridge globalen Amazon-Endpunkt bereit. Der Endpunkt kann die Verfügbarkeit Ihrer Anwendung verbessern, indem er sie regional fehlertolerant macht.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsEventsEventbus` Beschreibungen der `AwsEventsEventbus` Attribute finden Sie AwsEventsEventbusDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsEventsEventbus":
    "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
    "Name": "my-event-bus",
    "Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AllowAllAccountsFromOrganizationToPutEvents\",\"Effect\":\"Allow
\",\"Principal\":\"*\",\"Action\":\"events:PutEvents\",\"Resource\":
\"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\",\"Condition
\":{\"StringEquals\":{\"aws:PrincipalOrgID\":\"o-ki7yjtkjv5\"}}},{\"Sid\":
\"AllowAccountToManageRulesTheyCreated\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
\"arn:aws:iam::123456789012:root\"},\"Action\":[\"events:PutRule\",\"events:PutTargets
\",\"events:DeleteRule\",\"events:RemoveTargets\",\"events:DisableRule
\",\"events:EnableRule\",\"events:TagResource\",\"events:UntagResource\",
\"events:DescribeRule\",\"events:ListTargetsByRule\",\"events:ListTagsForResource\"],
\"Resource\":\"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\",\"Condition\":
{\"StringEqualsIfExists\":{\"events:creatorAccount\":\"123456789012\"}}}]}"
```

AwsGuardDuty

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsGuardDuty` Ressourcen.

AwsGuardDutyDetector

Das `AwsGuardDutyDetector` Objekt liefert Informationen über einen GuardDuty Amazon-Detektor. Ein Detektor ist ein Objekt, das den GuardDuty Service repräsentiert. Ein Detektor ist erforderlich GuardDuty , um betriebsbereit zu sein.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsGuardDutyDetector` Objekt. Beschreibungen der `AwsGuardDutyDetector` Attribute finden Sie AwsGuardDutyDetectorin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsGuardDutyDetector": {
    "FindingPublishingFrequency": "SIX_HOURS",
    "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Status": "ENABLED",
    "DataSources": {
        "CloudTrail": {
            "Status": "ENABLED"
        },
        "DnsLogs": {
            "Status": "ENABLED"
        },
        "FlowLogs": {
            "Status": "ENABLED"
        },
        "S3Logs": {
             "Status": "ENABLED"
         },
         "Kubernetes": {
             "AuditLogs": {
                "Status": "ENABLED"
             }
         },
         "MalwareProtection": {
             "ScanEc2InstanceWithFindings": {
                "EbsVolumes": {
                    "Status": "ENABLED"
                 }
             },
            "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-
protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
         }
    }
}
```

AwsIam

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsIam` Ressourcen.

AwsIamAccessKey

Das `AwsIamAccessKey` Objekt enthält Details zu einem IAM-Zugriffsschlüssel, der sich auf einen Befund bezieht.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsIamAccessKey` Objekt. Beschreibungen der `AwsIamAccessKey` Attribute finden Sie AwsIamAccessKeyDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsIamAccessKey": {
                        "AccessKeyId": "string",
                        "AccountId": "string",
                        "CreatedAt": "string",
                        "PrincipalId": "string",
                        "PrincipalName": "string",
                        "PrincipalType": "string",
                        "SessionContext": {
                            "Attributes": {
                                "CreationDate": "string",
                                "MfaAuthenticated": boolean
                            },
                            "SessionIssuer": {
                                "AccountId": "string",
                                "Arn": "string",
                                "PrincipalId": "string",
                                "Type": "string",
                                "UserName": "string"
                            }
                        },
                        "Status": "string"
                    }
```

AwsIamGroup

Das `AwsIamGroup` Objekt enthält Details zu einer IAM-Gruppe.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsIamGroup` Objekt. Beschreibungen der `AwsIamGroup` Attribute finden Sie AwsIamGroupDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsIamGroup": {
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleManagedAccess",
            "PolicyName": "ExampleManagedAccess",
        }
    ],
    "CreateDate": "2020-04-28T14:08:37.000Z",
    "GroupId": "AGPA4TPS3VLP7QEXAMPLE",
    "GroupName": "Example_User_Group",
    "GroupPolicyList": [
        {
            "PolicyName": "ExampleGroupPolicy"
        }
    ],
    "Path": "/"
}
```

AwsIamPolicy

Das `AwsIamPolicy` Objekt stellt eine IAM-Berechtigungsrichtlinie dar.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsIamPolicy` Objekt. Beschreibungen der `AwsIamPolicy` Attribute finden Sie AwsIamPolicyDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsIamPolicy": {
    "AttachmentCount": 1,
    "CreateDate": "2017-09-14T08:17:29.000Z",
    "DefaultVersionId": "v1",
    "Description": "Example IAM policy",
    "IsAttachable": true,
    "Path": "/",
    "PermissionsBoundaryUsageCount": 5,
    "PolicyId": "ANPAJ2UCCR6DPCEXAMPLE",
    "PolicyName": "EXAMPLE-MANAGED-POLICY",
    "PolicyVersionList": [
        {
            "VersionId": "v1",
            "IsDefaultVersion": true,
```

```
            "CreateDate": "2017-09-14T08:17:29.000Z"
        }
    ],
    "UpdateDate": "2017-09-14T08:17:29.000Z"
}
```

AwsIamRole

Das `AwsIamRole` Objekt enthält Informationen zu einer IAM-Rolle, einschließlich aller Richtlinien der Rolle.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsIamRole` Objekt. Beschreibungen der `AwsIamRole` Attribute finden Sie AwsIamRoleDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsIamRole": {
    "AssumeRolePolicyDocument": "{'Version': '2012-10-17','Statement': [{'Effect':
 'Allow','Action': 'sts:AssumeRole'}]}",
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExamplePolicy1",
            "PolicyName": "Example policy 1"
        },
        {
            "PolicyArn": "arn:aws:iam::444455556666:policy/ExamplePolicy2",
            "PolicyName": "Example policy 2"
        }
        ],
        "CreateDate": "2020-03-14T07:19:14.000Z",
        "InstanceProfileList": [
            {
                "Arn": "arn:aws:iam::333333333333:ExampleProfile",
                "CreateDate": "2020-03-11T00:02:27Z",
                "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
                "InstanceProfileName": "ExampleInstanceProfile",
                "Path": "/",
                "Roles": [
                    {
                       "Arn": "arn:aws:iam::444455556666:role/example-role",
                        "AssumeRolePolicyDocument": "",
                        "CreateDate": "2020-03-11T00:02:27Z",
```

```
                    "Path": "/",
                    "RoleId": "AROAJ52OTH4H7LEXAMPLE",
                    "RoleName": "example-role",
                }
            ]
        }
    ],
    "MaxSessionDuration": 3600,
    "Path": "/",
    "PermissionsBoundary": {
        "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
        "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
    },
    "RoleId": "AROA4TPS3VLEXAMPLE",
    "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
    "RolePolicyList": [
        {
            "PolicyName": "Example role policy"
        }
    ]
}
```

AwsIamUser

Das `AwsIamUser` Objekt stellt Informationen über einen Benutzer bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsIamUser` Objekt. Beschreibungen der `AwsIamUser` Attribute finden Sie AwsIamUserDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsIamUser": {
    "AttachedManagedPolicies": [
        {
            "PolicyName": "ExamplePolicy",
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleAccess"
        }
    ],
    "CreateDate": "2018-01-26T23:50:05.000Z",
    "GroupList": [],
    "Path": "/",
    "PermissionsBoundary" : {
```

```
        "PermissionsBoundaryArn" : "arn:aws:iam::aws:policy/AdministratorAccess",
        "PermissionsBoundaryType" : "PermissionsBoundaryPolicy"
    },
    "UserId": "AIDACKCEVSQ6C2EXAMPLE",
    "UserName": "ExampleUser",
    "UserPolicyList": [
        {
            "PolicyName": "InstancePolicy"
        }
    ]
}
```

AwsKinesis

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsKinesis` Ressourcen.

AwsKinesisStream

Das `AwsKinesisStream` Objekt enthält Details zu Amazon Kinesis Data Streams.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsKinesisStream` Objekt. Beschreibungen der `AwsKinesisStream` Attribute finden Sie AwsKinesisStreamDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsKinesisStream": {
 "Name": "test-vir-kinesis-stream",
 "Arn": "arn:aws:kinesis:us-east-1:293279581038:stream/test-vir-kinesis-stream",
 "RetentionPeriodHours": 24,
 "ShardCount": 2,
 "StreamEncryption": {
  "EncryptionType": "KMS",
  "KeyId": "arn:aws:kms:us-east-1:293279581038:key/849cf029-4143-4c59-91f8-
ea76007247eb"
 }
}
```

AwsKms

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsKms` Ressourcen.

AwsKmsKey

Das `AwsKmsKey` Objekt enthält Details zu einem AWS KMS key.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsKmsKey` Objekt. Beschreibungen der `AwsKmsKey` Attribute finden Sie AwsKmsKeyDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsKmsKey": {
                        "AWSAccountId": "string",
                        "CreationDate": "string",
                        "Description": "string",
                        "KeyId": "string",
                        "KeyManager": "string",
                        "KeyRotationStatus": boolean,
                        "KeyState": "string",
                        "Origin": "string"
                    }
```

AwsLambda

Im Folgenden finden Sie Beispiele für das AWS Security Finding-Format für `AwsLambda` Ressourcen.

AwsLambdaFunction

Das `AwsLambdaFunction` Objekt enthält Details zur Konfiguration einer Lambda-Funktion.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsLambdaFunction` Objekt. Beschreibungen der `AwsLambdaFunction` Attribute finden Sie AwsLambdaFunctionDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsLambdaFunction": {
    "Architectures": [
        "x86_64"
    ],
    "Code": {
        "S3Bucket": "DOC-EXAMPLE-BUCKET",
        "S3Key": "samplekey",
```

```
        "S3ObjectVersion": "2",
        "ZipFile": "myzip.zip"
    },
    "CodeSha256": "1111111111111abcdef",
    "DeadLetterConfig": {
        "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
    },
    "Environment": {
        "Variables": {
            "Stage": "foobar"
         },
        "Error": {
            "ErrorCode": "Sample-error-code",
            "Message": "Caller principal is a manager."
         }
     },
    "FunctionName": "CheckOut",
    "Handler": "main.py:lambda_handler",
    "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
    "LastModified": "2001-09-11T09:00:00Z",
    "Layers": {
        "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
        "CodeSize": 169
    },
    "PackageType": "Zip",
    "RevisionId": "23",
    "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
    "Runtime": "go1.7",
    "Timeout": 15,
    "TracingConfig": {
        "Mode": "Active"
    },
    "Version": "$LATEST$",
    "VpcConfig": {
        "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
         "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
    },
    "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
    "MemorySize": 2048
}
```

AwsLambdaLayerVersion

Das `AwsLambdaLayerVersion` Objekt enthält Details zu einer Lambda-Layer-Version.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsLambdaLayerVersion` Objekt. Beschreibungen der `AwsLambdaLayerVersion` Attribute finden Sie AwsLambdaLayerVersionDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsLambdaLayerVersion": {
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
    ],
    "CreatedDate": "2019-10-09T22:02:00.274+0000"
}
```

AwsMsk

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsMsk` Ressourcen.

AwsMskCluster

Das `AwsMskCluster` Objekt stellt Informationen über einen Amazon Managed Streaming for Apache Kafka (Amazon MSK) -Cluster bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsMskCluster` Beschreibungen der `AwsMskCluster` Attribute finden Sie AwsMskClusterDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsMskCluster": {
        "ClusterInfo": {
            "ClientAuthentication": {
                "Sasl": {
                    "Scram": {
                        "Enabled": true
                    },
                    "Iam": {
                        "Enabled": true
                    }
                },
                "Tls": {
```

```
                    "CertificateAuthorityArnList": [],
                    "Enabled": false
                },
                "Unauthenticated": {
                    "Enabled": false
                }
            },
            "ClusterName": "my-cluster",
            "CurrentVersion": "K2PWKAKR8XB7XF",
            "EncryptionInfo": {
                "EncryptionAtRest": {
                    "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                "EncryptionInTransit": {
                    "ClientBroker": "TLS",
                    "InCluster": true
                }
            },
            "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
            "NumberOfBrokerNodes": 3
        }
}
```

AwsNetworkFirewall

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsNetworkFirewall` Ressourcen.

AwsNetworkFirewallFirewall

Das `AwsNetworkFirewallFirewall` Objekt enthält Details zu einer AWS Network Firewall Firewall.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsNetworkFirewallFirewall` Objekt. Beschreibungen der `AwsNetworkFirewallFirewall` Attribute finden Sie AwsNetworkFirewallFirewallDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsNetworkFirewallFirewall": {
    "DeleteProtection": false,
```

```
    "FirewallArn": "arn:aws:network-firewall:us-east-1:024665936331:firewall/
testfirewall",
    "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
    "FirewallId": "dea7d8e9-ae38-4a8a-b022-672a830a99fa",
    "FirewallName": "testfirewall",
    "FirewallPolicyChangeProtection": false,
    "SubnetChangeProtection": false,
    "SubnetMappings": [
        {
            "SubnetId": "subnet-0183481095e588cdc"
        },
        {
            "SubnetId": "subnet-01f518fad1b1c90b0"
        }
    ],
    "VpcId": "vpc-40e83c38"
}
```

AwsNetworkFirewallFirewallPolicy

Das `AwsNetworkFirewallFirewallPolicy` Objekt enthält Details zu einer Firewall-Richtlinie. Eine Firewall-Richtlinie definiert das Verhalten einer Netzwerk-Firewall.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsNetworkFirewallFirewallPolicy` Objekt. Beschreibungen der `AwsNetworkFirewallFirewallPolicy` Attribute finden Sie AwsNetworkFirewallFirewallPolicyDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsNetworkFirewallFirewallPolicy": {
   "FirewallPolicy": {
    "StatefulRuleGroupReferences": [
        {
            "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/PatchesOnly"
        }
    ],
    "StatelessDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessRuleGroupReferences": [
       {
```

```
          "Priority": 1,
          "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1"
       }
     ]
   },
   "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
   "FirewallPolicyId": "9ceeda22-6050-4048-a0ca-50ce47f0cc65",
   "FirewallPolicyName": "InitialFirewall",
   "Description": "Initial firewall"
}
```

AwsNetworkFirewallRuleGroup

Das `AwsNetworkFirewallRuleGroup` Objekt enthält Details zu einer AWS Network Firewall Regelgruppe. Regelgruppen werden verwendet, um den Netzwerkverkehr zu untersuchen und zu kontrollieren. Zustandslose Regelgruppen gelten für einzelne Pakete. Stateful-Regelgruppen gelten für Pakete im Kontext ihres Datenverkehrs.

Auf Regelgruppen wird in Firewallrichtlinien verwiesen.

Die folgenden Beispiele zeigen das AWS Security Finding Format (ASFF) für das `AwsNetworkFirewallRuleGroup` Objekt. Beschreibungen der `AwsNetworkFirewallRuleGroup` Attribute finden Sie AwsNetworkFirewallRuleGroupDetailsin der AWS Security Hub API-Referenz.

Beispiel — Regelgruppe ohne Status

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 600,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1",
    "RuleGroupId": "fb13c4df-b6da-4c1e-91ec-84b7a5487493",
    "RuleGroupName": "Stateless-1"
    "Description": "Example of a stateless rule group",
    "Type": "STATELESS",
    "RuleGroup": {
        "RulesSource": {
            "StatelessRulesAndCustomActions": {
                "CustomActions": [],
                "StatelessRules": [
                    {
```

```
                        "Priority": 1,
                        "RuleDefinition": {
                            "Actions": [
                                "aws:pass"
                            ],
                            "MatchAttributes": {
                                "DestinationPorts": [
                                    {
                                        "FromPort": 443,
                                        "ToPort": 443
                                    }
                                ],
                                "Destinations": [
                                    {
                                        "AddressDefinition": "192.0.2.0/24"
                                    }
                                ],
                                "Protocols": [
                                           6
                                ],
                                "SourcePorts": [
                                    {
                                        "FromPort": 0,
                                        "ToPort": 65535
                                    }
                                ],
                                "Sources": [
                                    {
                                         "AddressDefinition": "198.51.100.0/24"
                                    }
                                ]
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Beispiel — Regelgruppe mit Status

```
"AwsNetworkFirewallRuleGroup": {
```

```
    "Capacity": 100,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/tupletest",
    "RuleGroupId": "38b71c12-da80-4643-a6c5-03337f8933e0",
    "RuleGroupName": "ExampleRuleGroup",
    "Description": "Example of a stateful rule group",
    "Type": "STATEFUL",
    "RuleGroup": {
        "RuleSource": {
            "StatefulRules": [
                {
                    "Action": "PASS",
                    "Header": {
                        "Destination": "Any",
                        "DestinationPort": "443",
                        "Direction": "ANY",
                        "Protocol": "TCP",
                        "Source": "Any",
                        "SourcePort": "Any"
                    },
                    "RuleOptions": [
                        {
                           "Keyword": "sid:1"
                        }
                    ]
                }
            ]
         }
    }
}
```

Im Folgenden finden Sie eine Liste mit Beispielen für gültige Werte für `AwsNetworkFirewallRuleGroup` Attribute:

- `Action`

  Zulässige Werte: `PASS` | `DROP` | `ALERT`

- `Protocol`

  Gültige Werte: `IP` `TCP` | `UDP` | `ICMP` | `HTTP` | `FTP` | `TLS` | `SMB` | `DNS` | `DCERPC` | `SSH` | `SMTP` | `IMAP` | `MSN` | `KRB5` | `IKEV2` | `TFTP` | `NTP` | `DHCP`

- `Flags`

Zulässige Werte: `FIN` | `SYN` | `RST` | `PSH` | `ACK` | `URG` | `ECE` | `CWR`

- `Masks`

  Zulässige Werte: `FIN` | `SYN` | `RST` | `PSH` | `ACK` | `URG` | `ECE` | `CWR`

AwsOpenSearchService

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsOpenSearchService` Ressourcen.

AwsOpenSearchServiceDomain

Das `AwsOpenSearchServiceDomain` Objekt enthält Informationen über eine Amazon OpenSearch Service-Domain.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsOpenSearchServiceDomain` Objekt. Beschreibungen der `AwsOpenSearchServiceDomain` Attribute finden Sie AwsOpenSearchServiceDomainDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsOpenSearchServiceDomain": {
    "AccessPolicies": "IAM_Id",
    "AdvancedSecurityOptions": {
        "Enabled": true,
        "InternalUserDatabaseEnabled": true,
        "MasterUserOptions": {
            "MasterUserArn": "arn:aws:iam::123456789012:user/third-master-use",
            "MasterUserName": "third-master-use",
            "MasterUserPassword": "some-password"
        }
    },
    "Arn": "arn:aws:Opensearch:us-east-1:111122223333:somedomain",
    "ClusterConfig": {
        "InstanceType": "c5.large.search",
        "InstanceCount": 1,
        "DedicatedMasterEnabled": true,
        "ZoneAwarenessEnabled": false,
        "ZoneAwarenessConfig": {
            "AvailabilityZoneCount": 2
        },
```

```
        "DedicatedMasterType": "c5.large.search",
        "DedicatedMasterCount": 3,
        "WarmEnabled": true,
        "WarmCount": 3,
        "WarmType": "ultrawarm1.large.search"
    },
    "DomainEndpoint": "https://es-2021-06-23t17-04-qowmgghud5vofgb5e4wmi.eu-
central-1.es.amazonaws.com",
    "DomainEndpointOptions": {
        "EnforceHTTPS": false,
        "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07",
        "CustomEndpointCertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/bda1bff1-79c0-49d0-abe6-50a15a7477d4",
        "CustomEndpointEnabled": true,
        "CustomEndpoint": "example.com"
    },
    "DomainEndpoints": {
        "vpc": "vpc-endpoint-h2dsd34efgyghrtguk5gt6j2foh4.us-east-1.es.amazonaws.com"
    },
    "DomainName": "my-domain",
    "EncryptionAtRestOptions": {
        "Enabled": false,
        "KmsKeyId": "1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a"
    },
    "EngineVersion": "7.1",
    "Id": "123456789012",
    "LogPublishingOptions": {
        "IndexSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-index-slow-logs",
            "Enabled": true
        },
        "SearchSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        },
        "AuditLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        }
    },
    "NodeToNodeEncryptionOptions": {
```

```
        "Enabled": true
    },
    "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "2022-04-28T14:08:37.000Z",
        "Cancellable": false,
        "CurrentVersion": "R20210331",
        "Description": "There is no software update available for this domain.",
        "NewVersion": "OpenSearch_1.0",
        "UpdateAvailable": false,
        "UpdateStatus": "COMPLETED",
        "OptionalDeployment": false
    },
    "VpcOptions": {
        "SecurityGroupIds": [
            "sg-2a3a4a5a"
        ],
        "SubnetIds": [
            "subnet-1a2a3a4a"
        ],
    }
}
```

AwsRds

Im Folgenden finden Sie Beispiele für das AWS Security Finding-Format für `AwsRds` Ressourcen.

AwsRdsDbCluster

Das `AwsRdsDbCluster` Objekt enthält Details zu einem Amazon RDS-Datenbankcluster.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsDbCluster` Objekt. Beschreibungen der `AwsRdsDbCluster` Attribute finden Sie AwsRdsDbClusterDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRdsDbCluster": {
    "ActivityStreamStatus": "stopped",
    "AllocatedStorage": 1,
    "AssociatedRoles": [
        {
        "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
        "Status": "PENDING"
```

```
        }
    ],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1c",
        "us-east-1e"
    ],
    "BackupRetentionPeriod": 1,
    "ClusterCreateTime": "2020-06-22T17:40:12.322Z",
    "CopyTagsToSnapshot": true,
    "CrossAccountClone": false,
    "CustomEndpoints": [],
    "DatabaseName": "Sample name",
    "DbClusterIdentifier": "database-3",
    "DbClusterMembers": [
        {
        "DbClusterParameterGroupStatus": "in-sync",
        "DbInstanceIdentifier": "database-3-instance-1",
        "IsClusterWriter": true,
        "PromotionTier": 1,
        }
    ],
    "DbClusterOptionGroupMemberships": [],
    "DbClusterParameterGroup": "cluster-parameter-group",
    "DbClusterResourceId": "cluster-example",
    "DbSubnetGroup": "subnet-group",
    "DeletionProtection": false,
    "DomainMemberships": [],
    "Status": "modifying",
    "EnabledCloudwatchLogsExports": [
        "audit",
        "error",
        "general",
        "slowquery"
    ],
    "Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
    "Engine": "aurora-mysql",
    "EngineMode": "provisioned",
    "EngineVersion": "5.7.mysql_aurora.2.03.4",
    "HostedZoneId": "ZONE1",
    "HttpEndpointEnabled": false,
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
```

```
    "MasterUsername": "admin",
    "MultiAz": false,
    "Port": 3306,
    "PreferredBackupWindow": "04:52-05:22",
    "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
    "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
    "ReadReplicaIdentifiers": [],
    "Status": "Modifying",
    "StorageEncrypted": true,
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example-1"
        }
    ],
}
```

AwsRdsDbClusterSnapshot

Das `AwsRdsDbClusterSnapshot` Objekt enthält Informationen über einen Amazon RDS-DB-Cluster-Snapshot.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsDbClusterSnapshot` Objekt. Beschreibungen der `AwsRdsDbClusterSnapshot` Attribute finden Sie AwsRdsDbClusterSnapshotDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRdsDbClusterSnaphot": {
    "AllocatedStorage": 0,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1d",
        "us-east-1e"
    ],
    "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
    "DbClusterIdentifier": "database-2",
    "DbClusterSnapshotAttributes": [{
        "AttributeName": "restore",
        "AttributeValues": ["123456789012"]
    }],
    "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
    "Engine": "aurora",
```

```
    "EngineVersion": "5.6.10a",
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "LicenseModel": "aurora",
    "MasterUsername": "admin",
    "PercentProgress": 100,
    "Port": 0,
    "SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
    "SnapshotType": "automated",
    "Status": "available",
    "StorageEncrypted": true,
    "VpcId": "vpc-faf7e380"
}
```

AwsRdsDbInstance

Das `AwsRdsDbInstance` Objekt enthält Details zu einer Amazon RDS-DB-Instance.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsDbInstance` Objekt. Beschreibungen der `AwsRdsDbInstance` Attribute finden Sie AwsRdsDbInstanceDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRdsDbInstance": {
    "AllocatedStorage": 20,
    "AssociatedRoles": [],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1d",
    "BackupRetentionPeriod": 7,
    "CaCertificateIdentifier": "certificate1",
    "CharacterSetName": "",
    "CopyTagsToSnapshot": true,
    "DbClusterIdentifier": "",
    "DbInstanceArn": "arn:aws:rds:us-east-1:111122223333:db:database-1",
    "DbInstanceClass": "db.t2.micro",
    "DbInstanceIdentifier": "database-1",
    "DbInstancePort": 0,
    "DbInstanceStatus": "available",
    "DbiResourceId": "db-EXAMPLE123",
    "DbName": "",
    "DbParameterGroups": [
        {
```

```
            "DbParameterGroupName": "default.mysql5.7",
            "ParameterApplyStatus": "in-sync"
        }
    ],
    "DbSecurityGroups": [],


    "DbSubnetGroup": {
        "DbSubnetGroupName": "my-group-123abc",
        "DbSubnetGroupDescription": "My subnet group",
        "VpcId": "vpc-example1",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-123abc",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1d"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-456def",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1c"
                },
                "SubnetStatus": "Active"
            }
      ],
        "DbSubnetGroupArn": ""
    },
    "DeletionProtection": false,
    "DomainMemberships": [],
    "EnabledCloudWatchLogsExports": [],
    "Endpoint": {
        "address": "database-1.example.us-east-1.rds.amazonaws.com",
        "port": 3306,
        "hostedZoneId": "ZONEID1"
    },
    "Engine": "mysql",
    "EngineVersion": "5.7.22",
    "EnhancedMonitoringResourceArn": "arn:aws:logs:us-east-1:111122223333:log-
group:Example:log-stream:db-EXAMPLE1",
    "IamDatabaseAuthenticationEnabled": false,
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
```

```
    "Iops": "",
    "KmsKeyId": "",
    "LatestRestorableTime": "2020-06-24T05:50:00.000Z",
    "LicenseModel": "general-public-license",
    "ListenerEndpoint": "",
    "MasterUsername": "admin",
    "MaxAllocatedStorage": 1000,
    "MonitoringInterval": 60,
    "MonitoringRoleArn": "arn:aws:iam::111122223333:role/rds-monitoring-role",
    "MultiAz": false,
    "OptionGroupMemberships": [
        {
            "OptionGroupName": "default:mysql-5-7",
            "Status": "in-sync"
        }
    ],
    "PreferredBackupWindow": "03:57-04:27",
    "PreferredMaintenanceWindow": "thu:10:13-thu:10:43",
    "PendingModifiedValues": {
        "DbInstanceClass": "",
        "AllocatedStorage": "",
        "MasterUserPassword": "",
        "Port": "",
        "BackupRetentionPeriod": "",
        "MultiAZ": "",
        "EngineVersion": "",
        "LicenseModel": "",
        "Iops": "",
        "DbInstanceIdentifier": "",
        "StorageType": "",
        "CaCertificateIdentifier": "",
        "DbSubnetGroupName": "",
        "PendingCloudWatchLogsExports": "",
        "ProcessorFeatures": []
    },
    "PerformanceInsightsEnabled": false,
    "PerformanceInsightsKmsKeyId": "",
    "PerformanceInsightsRetentionPeriod": "",
    "ProcessorFeatures": [],
    "PromotionTier": "",
    "PubliclyAccessible": false,
    "ReadReplicaDBClusterIdentifiers": [],
    "ReadReplicaDBInstanceIdentifiers": [],
    "ReadReplicaSourceDBInstanceIdentifier": "",
```

```
    "SecondaryAvailabilityZone": "",
    "StatusInfos": [],
    "StorageEncrypted": false,
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Timezone": "",
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-example1",
            "Status": "active"
        }
    ]
}
```

AwsRdsDbSecurityGroup

Das `AwsRdsDbSecurityGroup` Objekt enthält Informationen über einen Amazon Relational Database Service

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsDbSecurityGroup` Objekt. Beschreibungen der `AwsRdsDbSecurityGroup` Attribute finden Sie AwsRdsDbSecurityGroupDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRdsDbSecurityGroup": {
    "DbSecurityGroupArn": "arn:aws:rds:us-west-1:111122223333:secgrp:default",
    "DbSecurityGroupDescription": "default",
    "DbSecurityGroupName": "mysecgroup",
    "Ec2SecurityGroups": [
        {
          "Ec2SecurityGroupuId": "myec2group",
          "Ec2SecurityGroupName": "default",
          "Ec2SecurityGroupOwnerId": "987654321021",
          "Status": "authorizing"
        }
    ],
    "IpRanges": [
        {
          "Cidrip": "0.0.0.0/0",
          "Status": "authorizing"
        }
    ],
```

```
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234567f"
}
```

AwsRdsDbSnapshot

Das `AwsRdsDbSnapshot` Objekt enthält Details zu einem Amazon RDS-DB-Cluster-Snapshot.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsDbSnapshot` Objekt. Beschreibungen der `AwsRdsDbSnapshot` Attribute finden Sie AwsRdsDbSnapshotDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRdsDbSnapshot": {
    "DbSnapshotIdentifier": "rds:database-1-2020-06-22-17-41",
    "DbInstanceIdentifier": "database-1",
    "SnapshotCreateTime": "2020-06-22T17:41:29.967Z",
    "Engine": "mysql",
    "AllocatedStorage": 20,
    "Status": "available",
    "Port": 3306,
    "AvailabilityZone": "us-east-1d",
    "VpcId": "vpc-example1",
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "MasterUsername": "admin",
    "EngineVersion": "5.7.22",
    "LicenseModel": "general-public-license",
    "SnapshotType": "automated",
    "Iops": null,
    "OptionGroupName": "default:mysql-5-7",
    "PercentProgress": 100,
    "SourceRegion": null,
    "SourceDbSnapshotIdentifier": "",
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Encrypted": false,
    "KmsKeyId": "",
    "Timezone": "",
    "IamDatabaseAuthenticationEnabled": false,
    "ProcessorFeatures": [],
    "DbiResourceId": "db-resourceexample1"
}
```

AwsRdsEventSubscription

Das `AwsRdsEventSubscription` enthält Einzelheiten zu einem Abonnement für RDS-Ereignisbenachrichtigungen. Das Abonnement ermöglicht es RDS, Ereignisse zu einem SNS-Thema zu veröffentlichen.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRdsEventSubscription` Objekt. Beschreibungen der `AwsRdsEventSubscription` Attribute finden Sie AwsRdsEventSubscriptionDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRdsEventSubscription": {
    "CustSubscriptionId": "myawsuser-secgrp",
    "CustomerAwsId": "111111111111",
    "Enabled": true,
    "EventCategoriesList": [
        "configuration change",
        "failure"
    ],
    "EventSubscriptionArn": "arn:aws:rds:us-east-1:111111111111:es:my-instance-events",
    "SnsTopicArn": "arn:aws:sns:us-east-1:111111111111:myawsuser-RDS",
    "SourceIdsList": [
        "si-sample",
        "mysqldb-rr"
    ],
    "SourceType": "db-security-group",
    "Status": "creating",
    "SubscriptionCreationTime": "2021-06-27T01:38:01.090Z"
}
```

AwsRedshift

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsRedshift` Ressourcen.

AwsRedshiftCluster

Das `AwsRedshiftCluster` Objekt enthält Details zu einem Amazon Redshift Redshift-Cluster.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRedshiftCluster` Objekt. Beschreibungen der `AwsRedshiftCluster` Attribute finden Sie AwsRedshiftClusterDetailsin der AWS Security Hub API-Referenz.

Beispiel


```
"AwsRedshiftCluster": {
    "AllowVersionUpgrade": true,
    "AutomatedSnapshotRetentionPeriod": 1,
    "AvailabilityZone": "us-west-2d",
    "ClusterAvailabilityStatus": "Unavailable",
    "ClusterCreateTime": "2020-08-03T19:22:44.637Z",
    "ClusterIdentifier": "redshift-cluster-1",
    "ClusterNodes": [
        {
            "NodeRole": "LEADER",
            "PrivateIPAddress": "192.0.2.108",
            "PublicIPAddress": "198.51.100.29"
        },
        {
            "NodeRole": "COMPUTE-0",
            "PrivateIPAddress": "192.0.2.22",
            "PublicIPAddress": "198.51.100.63"
        },
        {
             "NodeRole": "COMPUTE-1",
             "PrivateIPAddress": "192.0.2.224",
             "PublicIPAddress": "198.51.100.226"
        }
        ],
    "ClusterParameterGroups": [
        {
            "ClusterParameterStatusList": [
                {
                    "ParameterName": "max_concurrency_scaling_clusters",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "enable_user_activity_logging",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "auto_analyze",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
```

```
                {
                    "ParameterName": "query_group",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "datestyle",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "extra_float_digits",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "search_path",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "statement_timeout",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "wlm_json_configuration",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "require_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "use_fips_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                }
            ],
            "ParameterApplyStatus": "in-sync",
            "ParameterGroupName": "temp"
        }
```

```
    ],
    "ClusterPublicKey": "JalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
    "ClusterRevisionNumber": 17498,
    "ClusterSecurityGroups": [
        {
            "ClusterSecurityGroupName": "default",
            "Status": "active"
        }
    ],
    "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "us-west-2",
        "ManualSnapshotRetentionPeriod": -1,
        "RetentionPeriod": 1,
        "SnapshotCopyGrantName": "snapshotCopyGrantName"
    },
    "ClusterStatus": "available",
    "ClusterSubnetGroupName": "default",
    "ClusterVersion": "1.0",
    "DBName": "dev",
    "DeferredMaintenanceWindows": [
        {
            "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
            "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
            "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
        }
     ],
    "ElasticIpStatus": {
        "ElasticIp": "203.0.113.29",
        "Status": "active"
    },
    "ElasticResizeNumberOfNodeOptions": "4",
    "Encrypted": false,
    "Endpoint": {
        "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
        "Port": 5439
    },
    "EnhancedVpcRouting": false,
    "ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
    "ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
    "HsmStatus": {
        "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
        "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
        "Status": "applying"
    },
```

```
    "IamRoles": [
        {
             "ApplyStatus": "in-sync",
             "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
        }
    ],
    "KmsKeyId": "kmsKeyId",
    "LoggingStatus": {
        "BucketName": "test-bucket",
        "LastFailureMessage": "test message",
        "LastFailureTime": "2020-08-09T13:00:00.000Z",
        "LastSuccessfulDeliveryTime": "2020-08-08T13:00:00.000Z",
        "LoggingEnabled": true,
        "S3KeyPrefix": "/"
    },
    "MaintenanceTrackName": "current",
    "ManualSnapshotRetentionPeriod": -1,
    "MasterUsername": "awsuser",
    "NextMaintenanceWindowStartTime": "2020-08-09T13:00:00.000Z",
    "NodeType": "dc2.large",
    "NumberOfNodes": 2,
    "PendingActions": [],
    "PendingModifiedValues": {
        "AutomatedSnapshotRetentionPeriod": 0,
        "ClusterIdentifier": "clusterIdentifier",
        "ClusterType": "clusterType",
        "ClusterVersion": "clusterVersion",
        "EncryptionType": "None",
        "EnhancedVpcRouting": false,
        "MaintenanceTrackName": "maintenanceTrackName",
        "MasterUserPassword": "masterUserPassword",
        "NodeType": "dc2.large",
        "NumberOfNodes": 1,
        "PubliclyAccessible": true
    },
    "PreferredMaintenanceWindow": "sun:13:00-sun:13:30",
    "PubliclyAccessible": true,
    "ResizeInfo": {
        "AllowCancelResize": true,
        "ResizeType": "ClassicResize"
    },
    "RestoreStatus": {
        "CurrentRestoreRateInMegaBytesPerSecond": 15,
        "ElapsedTimeInSeconds": 120,
```

```
        "EstimatedTimeToCompletionInSeconds": 100,
        "ProgressInMegaBytes": 10,
        "SnapshotSizeInMegaBytes": 1500,
        "Status": "restoring"
    },
    "SnapshotScheduleIdentifier": "snapshotScheduleIdentifier",
    "SnapshotScheduleState": "ACTIVE",
     "VpcId": "vpc-example",
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example"
        }
    ]
}
```

AwsRoute53

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsRoute53` Ressourcen.

AwsRoute53HostedZone

Das `AwsRoute53HostedZone` Objekt stellt Informationen über eine von Amazon Route 53 gehostete Zone bereit, einschließlich der vier Nameserver, die der Hosting-Zone zugewiesen sind. Eine gehostete Zone stellt eine Sammlung von Datensätzen dar, die zusammen verwaltet werden können und zu einem einzigen übergeordneten Domainnamen gehören.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsRoute53HostedZone` Objekt. Beschreibungen der `AwsRoute53HostedZone` Attribute finden Sie unter AwsRoute53 HostedZoneDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsRoute53HostedZone": {
    "HostedZone": {
        "Id": "Z06419652JEMGO9TA2XKL",
        "Name": "asff.testing",
        "Config": {
            "Comment": "This is an example comment."
        }
    },
```

```
    "NameServers": [
        "ns-470.awsdns-32.net",
        "ns-1220.awsdns-12.org",
        "ns-205.awsdns-13.com",
        "ns-1960.awsdns-51.co.uk"
    ],
    "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-
group:asfftesting:*",
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "HostedZoneId": "Z00932193AF5H180PPNZD"
        }
    },
    "Vpcs": [
        {
            "Id": "vpc-05d7c6e36bc03ea76",
            "Region": "us-east-1"
        }
    ]
}
```

AwsS3

Im Folgenden finden Sie Beispiele für das AWS Security Finding-Format für `AwsS3` Ressourcen.

AwsS3AccessPoint

`AwsS3AccessPoint`bietet Informationen über einen Amazon S3 S3-Zugriffspunkt. S3-Zugriffspunkte sind benannte Netzwerkendpunkte, die an S3-Buckets angeschlossen sind, mit denen Sie S3-Objektoperationen ausführen können.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsS3AccessPoint` Beschreibungen der *`AwsS3AccessPoint`* Attribute finden Sie unter awSS3 AccessPointDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsS3AccessPoint": {
        "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-
point",
        "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
```

```
        "Bucket": "DOC-EXAMPLE-BUCKET1",
        "BucketAccountId": "123456789012",
        "Name": "asff-access-point",
        "NetworkOrigin": "VPC",
        "PublicAccessBlockConfiguration": {
            "BlockPublicAcls": true,
            "BlockPublicPolicy": true,
            "IgnorePublicAcls": true,
            "RestrictPublicBuckets": true
        },
        "VpcConfiguration": {
            "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
        }
}
```

AwsS3AccountPublicAccessBlock

`AwsS3AccountPublicAccessBlock`bietet Informationen zur Amazon S3 Public Access Block-Konfiguration für Konten.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsS3AccountPublicAccessBlock` Objekt. Beschreibungen der *`AwsS3AccountPublicAccessBlock`* Attribute finden Sie unter awSS3 AccountPublicAccessBlockDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsS3AccountPublicAccessBlock": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": false,
    "RestrictPublicBuckets": true
}
```

AwsS3Bucket

Das `AwsS3Bucket` Objekt enthält Details zu einem Amazon S3 S3-Bucket.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsS3Bucket` Objekt. Beschreibungen der *`AwsS3Bucket`* Attribute finden Sie unter awSS3 BucketDetails in der AWS Security Hub API-Referenz.

Beispiel


```
"AwsS3Bucket": {
    "AccessControlList": "{\"grantSet\":null,\"grantList\":[{\"grantee\":{\"id\":
\"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\",\"displayName
\":null},\"permission\":\"FullControl\"},{\"grantee\":\"AllUsers\",\"permission\":
\"ReadAcp\"},{\"grantee\":\"AuthenticatedUsers\",\"permission\":\"ReadAcp\"}",,
    "BucketLifecycleConfiguration": {
       "Rules": [
           {
               "AbortIncompleteMultipartUpload": {
                   "DaysAfterInitiation": 5
               },
               "ExpirationDate": "2021-11-10T00:00:00.000Z",
               "ExpirationInDays": 365,
               "ExpiredObjectDeleteMarker": false,
               "Filter": {
                   "Predicate": {
                       "Operands": [
                           {
                               "Prefix": "tmp/",
                               "Type": "LifecyclePrefixPredicate"
                           },
                           {
                               "Tag": {
                                   "Key": "ArchiveAge",
                                   "Value": "9m"
                               },
                               "Type": "LifecycleTagPredicate"
                           }
                       ],
                       "Type": "LifecycleAndOperator"
                   }
               },
               "ID": "Move rotated logs to Glacier",
               "NoncurrentVersionExpirationInDays": -1,
               "NoncurrentVersionTransitions": [
                   {
                       "Days": 2,
                       "StorageClass": "GLACIER"
                   }
               ],
               "Prefix": "rotated/",
               "Status": "Enabled",
```

```
            "Transitions": [
                {
                    "Date": "2020-11-10T00:00:00.000Z",
                    "Days": 100,
                    "StorageClass": "GLACIER"
                }
            ]
        }
    ]
},
"BucketLoggingConfiguration": {
 "DestinationBucketName": "s3serversideloggingbucket-858726136312",
 "LogFilePrefix": "buckettestreadwrite23435/"
},
"BucketName": "DOC-EXAMPLE-BUCKET1",
"BucketNotificationConfiguration": {
 "Configurations": [{
  "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
  "Events": [
   "s3:ObjectCreated:Put"
  ],
  "Filter": {
   "S3KeyFilter": {
    "FilterRules": [
    {
     "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
     "Value": "pre"
    },
    {
     "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
     "Value": "suf"
    },
    ]
   }
  },
  "Type": "LambdaConfiguration"
 }]
},
"BucketVersioningConfiguration": {
 "IsMfaDeleteEnabled": true,
 "Status": "Off"
},
"BucketWebsiteConfiguration": {
 "ErrorDocument": "error.html",
```

```
      "IndexDocumentSuffix": "index.html",
      "RedirectAllRequestsTo": {
       "HostName": "example.com",
       "Protocol": "http"
      },
      "RoutingRules": [{
       "Condition": {
        "HttpErrorCodeReturnedEquals": "Redirected",
        "KeyPrefixEquals": "index"
          },
       "Redirect": {
        "HostName": "example.com",
        "HttpRedirectCode": "401",
        "Protocol": "HTTP",
        "ReplaceKeyPrefixWith": "string",
        "ReplaceKeyWith": "string"
       }
      }]
     },
     "CreatedAt": "2007-11-30T01:46:56.000Z",
     "ObjectLockConfiguration": {
      "ObjectLockEnabled": "Enabled",
      "Rule": {
       "DefaultRetention": {
        "Days": null,
        "Mode": "GOVERNANCE",
        "Years": 12
       },
      },
     },
     "OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
     "OwnerName": "s3bucketowner",
     "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": true,
         "BlockPublicPolicy": true,
         "IgnorePublicAcls": true,
         "RestrictPublicBuckets": true,
     },
     "ServerSideEncryptionConfiguration": {
         "Rules": [
             {
                 "ApplyServerSideEncryptionByDefault": {
                     "SSEAlgorithm": "AES256",
                     "KMSMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
```

```
                }
            }
        ]
    }
}
```

AwsS3Object

Das `AwsS3Object` Objekt stellt Informationen über ein Amazon S3 S3-Objekt bereit.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsS3Object` Objekt. Beschreibungen der *`AwsS3Object`* Attribute finden Sie unter awSS3 ObjectDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsS3Object": {
    "ContentType": "text/html",
    "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
    "LastModified": "2012-04-23T18:25:43.511Z",
    "ServerSideEncryption": "aws:kms",
    "SSEKMSKeyId": "arn:aws:kms:us-west-2:123456789012:key/4dff8393-e225-4793-
a9a0-608ec069e5a7",
    "VersionId": "ws31OurgOOjH_HHllIxPE35P.MELYaYh"
}
```

AwsSageMaker

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsSageMaker` Ressourcen.

AwsSageMakerNotebookInstance

Das `AwsSageMakerNotebookInstance` Objekt stellt Informationen über eine SageMaker Amazon-Notebook-Instance bereit, bei der es sich um eine Recheninstanz für maschinelles Lernen handelt, auf der die Jupyter Notebook App ausgeführt wird.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsSageMakerNotebookInstance` Beschreibungen der `AwsSageMakerNotebookInstance` Attribute finden Sie AwsSageMakerNotebookInstanceDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsSageMakerNotebookInstance": {
    "DirectInternetAccess": "Disabled",
    "InstanceMetadataServiceConfiguration": {
     "MinimumInstanceMetadataServiceVersion": "1",
    },
    "InstanceType": "ml.t2.medium",
    "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
    "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
    "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/
sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
    "NotebookInstanceName":
 "SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
    "NotebookInstanceStatus": "InService",
    "PlatformIdentifier": "notebook-al1-v1",
    "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-
SageMakerCustomExecution-1R0X32HGC38IW",
    "RootAccess": "Disabled",
    "SecurityGroups": [
     "sg-06b347359ab068745"
    ],
    "SubnetId": "subnet-02c0deea5fa64578e",
    "Url":
 "sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-
east-1.sagemaker.aws",
    "VolumeSizeInGB": 5
}
```

AwsSecretsManager

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsSecretsManager` Ressourcen.

AwsSecretsManagerSecret

Das `AwsSecretsManagerSecret` Objekt enthält Details zu einem Secrets Manager Manager-Geheimnis.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsSecretsManagerSecret` Objekt. Beschreibungen der `AwsSecretsManagerSecret` Attribute finden Sie AwsSecretsManagerSecretDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsSecretsManagerSecret": {
    "RotationRules": {
        "AutomaticallyAfterDays": 30
    },
    "RotationOccurredWithinFrequency": true,
    "KmsKeyId": "kmsKeyId",
    "RotationEnabled": true,
    "RotationLambdaArn": "arn:aws:lambda:us-
west-2:777788889999:function:MyTestRotationLambda",
    "Deleted": false,
    "Name": "MyTestDatabaseSecret",
    "Description": "My test database secret"
}
```

AwsSns

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsSns` Ressourcen.

AwsSnsTopic

Das `AwsSnsTopic` Objekt enthält Details zu einem Thema von Amazon Simple Notification Service.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsSnsTopic` Objekt. Beschreibungen der `AwsSnsTopic` Attribute finden Sie AwsSnsTopicDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsSnsTopic": {
    "ApplicationSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
ApplicationSuccessFeedbackRoleArn",
    "FirehoseFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseFailureFeedbackRoleArn",
    "FirehoseSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseSuccessFeedbackRoleArn",
    "HttpFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpFailureFeedbackRoleArn",
    "HttpSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpSuccessFeedbackRoleArn",
    "KmsMasterKeyId": "alias/ExampleAlias",
    "Owner": "123456789012",
    "SqsFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsFailureFeedbackRoleArn",
```

```
    "SqsSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsSuccessFeedbackRoleArn",
    "Subscription": {
         "Endpoint": "http://sampleendpoint.com",
         "Protocol": "http"
    },
    "TopicName": "SampleTopic"
}
```

AwsSqs

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsSqs` Ressourcen.

AwsSqsQueue

Das `AwsSqsQueue` Objekt enthält Informationen über eine Amazon Simple Queue Service-Warteschlange.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsSqsQueue` Objekt. Beschreibungen der `AwsSqsQueue` Attribute finden Sie AwsSqsQueueDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsSqsQueue": {
    "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
    "KmsDataKeyReusePeriodSeconds": 60,,
    "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "QueueName": "sample-queue"
}
```

AwsSsm

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsSsm` Ressourcen.

AwsSsmPatchCompliance

Das `AwsSsmPatchCompliance` Objekt stellt Informationen über den Status eines Patches auf einer Instanz bereit, basierend auf der Patch-Baseline, die zum Patchen der Instanz verwendet wurde.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsSsmPatchCompliance` Objekt. Beschreibungen der `AwsSsmPatchCompliance` Attribute finden Sie AwsSsmPatchComplianceDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsSsmPatchCompliance": {
    "Patch": {
        "ComplianceSummary": {
            "ComplianceType": "Patch",
            "CompliantCriticalCount": 0,
            "CompliantHighCount": 0,
            "CompliantInformationalCount": 0,
            "CompliantLowCount": 0,
            "CompliantMediumCount": 0,
            "CompliantUnspecifiedCount": 461,
            "ExecutionType": "Command",
            "NonCompliantCriticalCount": 0,
            "NonCompliantHighCount": 0,
            "NonCompliantInformationalCount": 0,
            "NonCompliantLowCount": 0,
            "NonCompliantMediumCount": 0,
            "NonCompliantUnspecifiedCount": 0,
            "OverallSeverity": "UNSPECIFIED",
            "PatchBaselineId": "pb-0c5b2769ef7cbe587",
            "PatchGroup": "ExamplePatchGroup",
            "Status": "COMPLIANT"
        }
    }
}
```

AwsStepFunctions

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsStepFunctions` Ressourcen.

AwsStepFunctionStateMachine

Das `AwsStepFunctionStateMachine` Objekt stellt Informationen über eine AWS Step Functions Zustandsmaschine bereit. Dabei handelt es sich um einen Workflow, der aus einer Reihe von ereignisgesteuerten Schritten besteht.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsStepFunctionStateMachine` Beschreibungen der `AwsStepFunctionStateMachine` Attribute finden Sie AwsStepFunctionStateMachinein der AWS Security Hub API-Referenz.

Beispiel

```
"AwsStepFunctionStateMachine": {
    "StateMachineArn": "arn:aws:states:us-
east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-
fQLujTeXvwsb",
    "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
    "Status": "ACTIVE",
    "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-
StatesExecutionRole-1PNM71RVO1UKT",
    "Type": "STANDARD",
    "LoggingConfiguration": {
        "Level": "OFF",
        "IncludeExecutionData": false
    },
    "TracingConfiguration": {
        "Enabled": false
    }
}
```

AwsWaf

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsWaf` Ressourcen.

AwsWafRateBasedRule

Das `AwsWafRateBasedRule` Objekt enthält Details zu einer AWS WAF ratenbasierten Regel für globale Ressourcen. Eine AWS WAF ratenbasierte Regel bietet Einstellungen, mit denen angegeben wird, wann eine Anfrage zugelassen, blockiert oder gezählt werden soll. Ratenbasierte Regeln beinhalten die Anzahl der Anfragen, die über einen bestimmten Zeitraum eingehen.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsWafRateBasedRule` Beschreibungen der `AwsWafRateBasedRule` Attribute finden Sie AwsWafRateBasedRuleDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
```

```
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRateBasedRule

Das `AwsWafRegionalRateBasedRule` Objekt enthält Details zu einer ratenbasierten Regel für regionale Ressourcen. Eine ratenbasierte Regel bietet Einstellungen, mit denen angegeben wird, wann eine Anfrage zugelassen, blockiert oder gezählt werden soll. Ratenbasierte Regeln beinhalten die Anzahl der Anfragen, die über einen bestimmten Zeitraum eingehen.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das Objekt. `AwsWafRegionalRateBasedRule` Beschreibungen der `AwsWafRegionalRateBasedRule` Attribute finden Sie AwsWafRegionalRateBasedRuleDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRegionalRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRule

Das `AwsWafRegionalRule` Objekt enthält Details zu einer AWS WAF regionalen Regel. Diese Regel identifiziert die Webanfragen, die Sie zulassen, blockieren oder zählen möchten.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafRegionalRule` Objekt. Beschreibungen der `AwsWafRegionalRule` Attribute finden Sie AwsWafRegionalRuleDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRegionalRule": {
    "MetricName": "SampleWAF_Rule__Metric_1",
    "Name": "bb-waf-regional-rule-not-empty-conditions-compliant",
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de95fe",
    "PredicateList": [{
        "DataId": "127d9346-e607-4e93-9286-c1296fb5445a",
        "Negated": false,
        "Type": "GeoMatch"
    }]
}
```

AwsWafRegionalRuleGroup

Das `AwsWafRegionalRuleGroup` Objekt enthält Details zu einer AWS WAF regionalen Regelgruppe. Eine Regelgruppe ist eine Sammlung vordefinierter Regeln, die Sie einer Web-Zugriffskontrollliste (Web-ACL) hinzufügen.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafRegionalRuleGroup` Objekt. Beschreibungen der `AwsWafRegionalRuleGroup` Attribute finden Sie AwsWafRegionalRuleGroupDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRegionalRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFClassicRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW"
        }
    }],
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
}
```

AwsWafRegionalWebAcl

`AwsWafRegionalWebAcl`enthält Einzelheiten zu einer AWS WAF regionalen Web-Zugriffskontrollliste (Web Access Control List, Web-ACL). Eine Web-ACL enthält die Regeln, die die Anfragen identifizieren, die Sie zulassen, blockieren oder zählen möchten.

Im Folgenden finden Sie ein Beispiel für einen `AwsWafRegionalWebAcl` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsApiGatewayV2Stage` Attribute finden Sie AwsWafRegionalWebAclDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRegionalWebAcl": {
    "DefaultAction": "ALLOW",
    "MetricName" : "web-regional-webacl-metric-1",
    "Name": "WebACL_123",
    "RulesList": [
        {
            "Action": {
                "Type": "Block"
            },
            "Priority": 3,
            "RuleId": "24445857-852b-4d47-bd9c-61f05e4d223c",
            "Type": "REGULAR",
            "ExcludedRules": [
                {
                    "ExclusionType": "Exclusion",
                    "RuleId": "Rule_id_1"
                }
            ],
            "OverrideAction": {
                "Type": "OVERRIDE"
            }
        }
    ],
    "WebAclId": "443c76f4-2e72-4c89-a2ee-389d501c1f67"
}
```

AwsWafRule

`AwsWafRule`stellt Informationen zu einer AWS WAF Regel bereit. Eine AWS WAF Regel identifiziert die Webanfragen, die Sie zulassen, blockieren oder zählen möchten.

Im Folgenden finden Sie ein Beispiel für einen `AwsWafRule` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsApiGatewayV2Stage` Attribute finden Sie AwsWafRuleDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRule": {
    "MetricName": "AwsWafRule_Metric_1",
    "Name": "AwsWafRule_Name_1",
    "PredicateList": [{
        "DataId": "cdd225da-32cf-4773-1dc2-3bca3ed9c19c",
        "Negated": false,
        "Type": "GeoMatch"
    }],
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de953e"
}
```

AwsWafRuleGroup

`AwsWafRuleGroup`stellt Informationen zu einer AWS WAF Regelgruppe bereit. Eine AWS WAF Regelgruppe ist eine Sammlung vordefinierter Regeln, die Sie einer Web-Zugriffskontrollliste (Web-ACL) hinzufügen.

Im Folgenden finden Sie ein Beispiel für einen `AwsWafRuleGroup` Befund im AWS Security Finding Format (ASFF). Beschreibungen der `AwsApiGatewayV2Stage` Attribute finden Sie AwsWafRuleGroupDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW",
        },
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
    }]
}
```

AwsWafv2RuleGroup

Das `AwsWafv2RuleGroup` Objekt enthält Details zu einer AWS WAF V2-Regelgruppe.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafv2RuleGroup` Objekt. Beschreibungen der `AwsWafv2RuleGroup` Attribute finden Sie unter AwsWafv2 RuleGroupDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafv2RuleGroup": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1000,
    "Description": "Resource for ASFF",
    "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "wafv2rulegroupasff",
    "Rules": [{
     "Action": {
     "Allow": {
      "CustomRequestHandling": {
       "InsertHeaders": [
        {
        "Name": "AllowActionHeader1Name",
        "Value": "AllowActionHeader1Value"
        },
        {
        "Name": "AllowActionHeader2Name",
        "Value": "AllowActionHeader2Value"
        }
       ]
      }
     },
     "Name": "RuleOne",
     "Priority": 1,
     "VisibilityConfig": {
      "CloudWatchMetricsEnabled": true,
      "MetricName": "rulegroupasff",
      "SampledRequestsEnabled": false
     }
    }],
    "VisibilityConfig": {
     "CloudWatchMetricsEnabled": true,
```

```
      "MetricName": "rulegroupasff",
      "SampledRequestsEnabled": false
    }
}
```

AwsWafWebAcl

Das `AwsWafWebAcl` Objekt enthält Details zu einer AWS WAF Web-ACL.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafWebAcl` Objekt. Beschreibungen der `AwsWafWebAcl` Attribute finden Sie AwsWafWebAclDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafWebAcl": {
    "DefaultAction": "ALLOW",
    "Name": "MyWafAcl",
    "Rules": [
        {
            "Action": {
                "Type": "ALLOW"
            },
            "ExcludedRules": [
                {
                    "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"
                }
            ],
            "OverrideAction": {
                "Type": "NONE"
            },
            "Priority": 1,
            "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98",
            "Type": "REGULAR"
        }
    ],
    "WebAclId": "waf-1234567890"
}
```

AwsWafv2WebAcl

Das `AwsWafv2WebAcl` Objekt enthält Details zu einer AWS WAF V2-Web-ACL.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsWafv2WebAcl` Objekt. Beschreibungen der `AwsWafv2WebAcl` Attribute finden Sie unter AwsWafv2 WebAclDetails in der AWS Security Hub API-Referenz.

Beispiel

```
"AwsWafv2WebAcl": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1326,
    "CaptchaConfig": {
     "ImmunityTimeProperty": {
      "ImmunityTime": 500
     }
    },
    "DefaultAction": {
     "Block": {}
    },
    "Description": "Web ACL for JsonBody testing",
    "ManagedbyFirewallManager": false,
    "Name": "WebACL-RoaD4QexqSxG",
    "Rules": [{
     "Action": {
      "RuleAction": {
       "Block": {}
      }
     },
     "Name": "TestJsonBodyRule",
     "Priority": 1,
     "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "JsonBodyMatchMetric"
     }
    }],
    "VisibilityConfig": {
     "SampledRequestsEnabled": true,
     "CloudWatchMetricsEnabled": true,
     "MetricName": "TestingJsonBodyMetric"
    }
}
```

AwsXray

Im Folgenden finden Sie Beispiele für das AWS Security Finding Format für `AwsXray` Ressourcen.

AwsXrayEncryptionConfig

Das `AwsXrayEncryptionConfig` Objekt enthält Informationen zur Verschlüsselungskonfiguration für AWS X-Ray.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `AwsXrayEncryptionConfig` Objekt. Beschreibungen der `AwsXrayEncryptionConfig` Attribute finden Sie AwsXrayEncryptionConfigDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"AwsXRayEncryptionConfig":{
    "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
    "Status": "UPDATING",
    "Type":"KMS"
}
```

Container

Container-Details, die mit einem Fund zusammenhängen.

Das folgende Beispiel zeigt das AWS Security Finding Format (ASFF) für das `Container` Objekt. Beschreibungen der `Container` Attribute finden Sie ContainerDetailsin der AWS Security Hub API-Referenz.

Beispiel

```
"Container": {
    "ContainerRuntime": "docker",
    "ImageId": "image12",
    "ImageName": "1111111/
knotejs@sha256:372131c9fef111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "Name": "knote",
    "Privileged": true,
    "VolumeMounts": [{
        "Name": "vol-03909e9",
        "MountPath": "/mnt/etc"
```

```
    }]
}
```

Other

Mit dem `Other` Objekt können Sie benutzerdefinierte Felder und Werte angeben. Sie verwenden das `Other` Objekt in den folgenden Fällen.

- Der Ressourcentyp hat kein entsprechendes `Details` Objekt. Um Details für die Ressource bereitzustellen, verwenden Sie das `Other` Objekt.
- Das `Details` Objekt für den Ressourcentyp enthält nicht alle Attribute, die Sie auffüllen möchten. Verwenden Sie in diesem Fall das `Details` Objekt für den Ressourcentyp, um die verfügbaren Attribute aufzufüllen. Verwenden Sie das `Other` Objekt, um die Attribute aufzufüllen, die sich nicht im typspezifischen Objekt befinden.
- Der Ressourcentyp gehört nicht zu den angegebenen Typen. In diesem Fall legen Sie `Resource.Type` auf fest und verwenden das `Other` Objekt`Other`, um die Details aufzufüllen.

Typ: Karte mit bis zu 50 Schlüssel-Wert-Paaren

Jedes Schlüssel-Wert-Paar muss die folgenden Anforderungen erfüllen.

- Der Schlüssel muss weniger als 128 Zeichen enthalten.
- Der Wert muss weniger als 1.024 Zeichen enthalten.

Einblicke in AWS Security Hub

Ein AWS Security Hub Hub-Einblick ist eine Sammlung verwandter Ergebnisse. Es identifiziert einen Sicherheitsbereich, der Aufmerksamkeit und Intervention erfordert. Ein Insight könnte beispielsweise auf EC2-Instances hinweisen, die Gegenstand von Ergebnissen sind, die auf schlechte Sicherheitspraktiken hinweisen. Ein Insight bringt Ergebnisse von verschiedenen Ergebnis-Anbietern zusammen.

Jedes Insight wird von einer Gruppe durch Anweisung und optionale Filter definiert. Die Gruppe nach Anweisung gibt an, wie die übereinstimmenden Ergebnisse gruppiert werden sollen, und identifiziert den Elementtyp, für den das Insight gilt. Wenn beispielsweise ein Insight nach Ressourcenbezeichner gruppiert ist, erstellt das Insight eine Liste von Ressourcenbezeichnern. Die optionalen Filter identifizieren die passenden Ergebnisse für den Einblick. Beispielsweise möchten Sie möglicherweise nur Ergebnisse von bestimmten Anbietern oder Ergebnisse sehen, die mit bestimmten Ressourcentypen verknüpft sind.

Security Hub bietet mehrere integrierte verwaltete Einblicke. Verwaltete Insights können nicht geändert oder gelöscht werden.

Um Sicherheitsprobleme zu verfolgen, die für Ihre AWS Umgebung und Nutzung spezifisch sind, können Sie benutzerdefinierte Einblicke erstellen.

Ein Insight liefert nur dann Ergebnisse, wenn Sie Integrationen oder Standards aktiviert haben, die zu passenden Ergebnissen führen. Zum Beispiel der verwaltete Einblick 29. Ressourcen mit der höchsten Anzahl fehlgeschlagener CIS-Prüfungen geben nur dann Ergebnisse zurück, wenn Sie den AWS CIS-Foundations-Standard aktivieren.

Themen

Liste der Erkenntnisse anzeigen und filtern

Auf der Insights-Seite wird die Liste der verfügbaren Erkenntnisse angezeigt.

Standardmäßig werden in der Liste sowohl verwaltete als auch benutzerdefinierte Erkenntnisse angezeigt. Um die Insight-Liste nach dem Insight-Typ zu filtern, wählen Sie den Insight-Typ aus dem Drop-down-Menü, das sich neben dem Filterfeld befindet.

- Um alle verfügbaren Erkenntnisse anzuzeigen, wählen Sie Alle Erkenntnisse aus. Dies ist die Standardoption.
- Um nur verwaltete Einblicke anzuzeigen, wählen Sie Security Hub Managed Insights.
- Um nur benutzerdefinierte Einblicke anzuzeigen, wählen Sie Benutzerdefinierte Einblicke.

Sie können die Insight-Liste auch nach dem Text im Insight-Namen filtern.

Geben Sie in das Filterfeld den Text ein, der zum Filtern der Liste verwendet werden soll. Der Filter unterscheidet nicht zwischen Groß- und Kleinschreibung. Der Filter sucht nach Erkenntnissen, die den Text an einer beliebigen Stelle im Insight-Namen enthalten.

Anzeigen von Insight-Ergebnissen und -Resultaten und Ergreifen geeigneter Maßnahmen

Für jeden Einblick ermittelt AWS Security Hub zunächst die Ergebnisse, die den Filterkriterien entsprechen, und verwendet dann das Gruppierungsattribut, um die übereinstimmenden Ergebnisse zu gruppieren.

Auf der Insights-Konsolenseite können Sie die Ergebnisse und Ergebnisse einsehen und entsprechende Maßnahmen ergreifen.

Wenn Sie die regionsübergreifende Aggregation aktivieren, enthalten die Ergebnisse für verwaltete Erkenntnisse in der Aggregationsregion Ergebnisse aus der Aggregationsregion und den verknüpften Regionen. Wenn die Erkenntnisse bei benutzerdefinierten Insight-Ergebnissen nicht nach Region gefiltert werden, enthalten die Ergebnisse Ergebnisse aus der Aggregationsregion und den verknüpften Regionen.

In anderen Regionen beziehen sich die Insight-Ergebnisse nur auf diese Region.

Informationen zur Konfiguration der regionsübergreifenden Aggregation finden Sie unter. Regionsübergreifende Aggregation

Insight-Ergebnisse anzeigen und entsprechende Maßnahmen ergreifen (Konsole)

Die Insight-Ergebnisse bestehen aus einer gruppierten Liste der Ergebnisse für den Insight. Wenn die Erkenntnisse beispielsweise nach Ressourcen-Identifikatoren gruppiert sind, dann sind die Insight-Ergebnisse die Liste der Ressourcen-Identifikatoren. Jedes Element in der Ergebnisliste gibt die Anzahl der übereinstimmenden Ergebnisse für dieses Element an.

Beachten Sie, dass, wenn die Ergebnisse nach Ressourcen-ID oder Ressourcentyp gruppiert sind, die Ergebnisse alle Ressourcen enthalten, die in den entsprechenden Ergebnissen enthalten sind. Dies schließt Ressourcen ein, deren Typ sich von dem in den Filterkriterien angegebenen Ressourcentyp unterscheidet. Ein Insight identifiziert beispielsweise Ergebnisse, die mit S3-Buckets verknüpft sind. Wenn ein übereinstimmendes Ergebnis sowohl eine S3-Bucket-Ressource als auch eine IAM-Zugriffsschlüsselressource enthält, werden in den Insight-Ergebnissen beide Ressourcen aufgeführt.

Die Ergebnisliste ist von den meisten bis zu den wenigsten übereinstimmenden Ergebnissen sortiert.

Security Hub kann nur 100 Ergebnisse anzeigen. Wenn es mehr als 100 Gruppierungswerte gibt, werden nur die ersten 100 angezeigt.

Zusätzlich zur Ergebnisliste wird in den Insight-Ergebnissen eine Reihe von Diagrammen angezeigt, die die Anzahl der übereinstimmenden Ergebnisse für die folgenden Attribute zusammenfassen.

- Bezeichnung des Schweregrads — Anzahl der Ergebnisse für jeden Schweregrad
- AWS-Konto ID — Die fünf wichtigsten Konto-IDs für die entsprechenden Ergebnisse
- Ressourcentyp — Die fünf wichtigsten Ressourcentypen für die passenden Ergebnisse
- Ressourcen-ID — Die fünf wichtigsten Ressourcen-IDs für die passenden Ergebnisse
- Produktname — Die fünf besten Anbieter für die Suche nach den passenden Ergebnissen

Wenn Sie benutzerdefinierte Aktionen konfiguriert haben, können Sie ausgewählte Ergebnisse an eine benutzerdefinierte Aktion senden. Die Aktion muss mit einer CloudWatch Regel für den `Security Hub Insight Results` Ereignistyp verknüpft sein. Siehe the section called “Automatisierte Reaktion und Problembehebung”.

Wenn Sie keine benutzerdefinierten Aktionen konfiguriert haben, ist das Aktionsmenü deaktiviert.

So zeigen Sie die Liste der Insight-Ergebnisse an und ergreifen Maßnahmen.

1. Öffnen Sie die AWS Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Insights aus.
3. Um die Liste der Insight-Ergebnisse anzuzeigen, wählen Sie den Insight-Namen aus.
4. Wählen Sie das Kontrollkästchen für jedes Ergebnis, das an die benutzerdefinierte Aktion gesendet werden soll.
5. Wählen Sie im Menü Actions (Aktionen) die benutzerdefinierte Aktion aus.

Insight-Ergebnisse anzeigen (Security Hub Hub-API, AWS CLI)

Um Insight-Ergebnisse anzuzeigen, können Sie einen API-Aufruf oder den verwenden AWS Command Line Interface.

Um Insight-Ergebnisse anzuzeigen (Security Hub Hub-API, AWS CLI)

- Security Hub Hub-API — Verwenden Sie den `GetInsightResults`Vorgang. Um die Erkenntnisse zu identifizieren, für die Ergebnisse zurückgegeben werden sollen, benötigen Sie den Insight-ARN. Verwenden Sie die `GetInsights`Operation, um die Insight-ARNs für benutzerdefinierte Erkenntnisse zu erhalten.
- AWS CLI— Führen Sie den Befehl in der `get-insight-results`Befehlszeile aus.

```
aws securityhub get-insight-results --insight-arn <insight ARN>
```

Beispiel:

```
aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Ergebnisse anzeigen, um ein Insight-Ergebnis zu erhalten (Konsole)

In der Ergebnisliste des Insights können Sie die Liste der Ergebnisse für jedes Resultat anzeigen.

So zeigen Sie Insight-Ergebnisse an und ergreifen Maßnahmen:

1. Öffnen Sie die AWS Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Insights aus.
3. Um die Liste der Insight-Ergebnisse anzuzeigen, wählen Sie den Insight-Namen aus.
4. Um die Liste der Ergebnisse für ein Insight-Ergebnis anzuzeigen, wählen Sie das Element aus der Ergebnisliste aus.

Die Ergebnisliste zeigt die aktiven Ergebnisse für das ausgewählte Insight-Ergebnis mit dem Workflow-Status `NEW` oder `NOTIFIED`.

In der Ergebnisliste können Sie die folgenden Aktionen ausführen.

- Ändern der Filter und Gruppierung für die Liste
- Anzeigen der Details für einzelne Ergebnisse
- Aktualisieren des Workflow-Status der Ergebnisse
- Senden der Ergebnisse an benutzerdefinierte Aktionen

Verwaltete Insights

AWSSecurity Hub bietet mehrere verwaltete Einblicke.

Sie können von Security Hub verwaltete Einblicke nicht bearbeiten oder löschen. Sie können die Insight-Ergebnisse und -Resultate einsehen und Maßnahmen ergreifen. Sie können auch einen verwalteten Insight als Grundlage für einen neuen benutzerdefinierten Insight verwenden.

Wie bei allen Insights gibt ein verwalteter Insight nur Ergebnisse zurück, wenn Sie Produktintegrationen oder Sicherheitsstandards aktiviert haben, die zu passenden Ergebnissen führen können.

Bei Erkenntnissen, die nach Ressourcen-IDs gruppiert sind, enthalten die Ergebnisse die Identifikatoren aller Ressourcen in den entsprechenden Ergebnissen. Dazu gehören Ressourcen, deren Typ sich von dem in den Filterkriterien angegebenen Ressourcentyp unterscheidet. Insight 2 identifiziert beispielsweise Ergebnisse, die mit Amazon S3 S3-Buckets verknüpft sind. Wenn ein übereinstimmendes Ergebnis sowohl eine S3-Bucket-Ressource als auch eine IAM-Zugriffsschlüsselressource enthält, umfassen die Insight-Ergebnisse beide Ressourcen.

Security Hub bietet die folgenden verwalteten Einblicke:

1. AWS-Ressourcen mit den meisten Ergebnissen

   ARN: `arn:aws:securityhub:::insight/securityhub/default/1`

   Gruppiert nach: Ressourcen-ID

   Filter finden:

   - Datensatzstatus ist `ACTIVE`
   - Workflow-Status ist `NEW` oder `NOTIFIED`

2. S3-Buckets mit öffentlichen Lese- oder Schreibberechtigungen

   ARN: `arn:aws:securityhub:::insight/securityhub/default/10`

   Gruppiert nach: Ressourcen-ID

   Filter finden:

   - Typ beginnt mit `Effects/Data Exposure`
   - Ressourcentyp ist `AwsS3Bucket`
   - Datensatzstatus ist `ACTIVE`
   - Workflow-Status ist `NEW` oder `NOTIFIED`

3. AMIs, die die meisten Ergebnisse erzeugen

   ARN: `arn:aws:securityhub:::insight/securityhub/default/3`

   Gruppiert nach: Image-ID der EC2-Instanz

   Filter finden:

   - Ressourcentyp ist `AwsEc2Instance`
   - Datensatzstatus ist `ACTIVE`
   - Workflow-Status ist `NEW` oder `NOTIFIED`

4. EC2-Instances, die mit bekannten Taktiken, Techniken und Verfahren (Tactics, Techniques and Procedures, TTPs) zusammenhängen

   ARN: `arn:aws:securityhub:::insight/securityhub/default/14`

   Gruppiert nach: Ressourcen-ID

Filter finden:

- Typ beginnt mit `TTPs`
- Ressourcentyp ist `AwsEc2Instance`
- Datensatzstatus ist `ACTIVE`
- Workflow-Status ist `NEW` oder `NOTIFIED`

5. AWSPrincipals mit verdächtiger Zugriffsschlüsselaktivität

ARN: `arn:aws:securityhub:::insight/securityhub/default/9`

Gruppiert nach: Prinzipalname des IAM-Zugriffsschlüssels

Filter finden:

- Ressourcentyp ist `AwsIamAccessKey`
- Datensatzstatus ist `ACTIVE`
- Workflow-Status ist `NEW` oder `NOTIFIED`

6. AWS-Ressourcen-Instances, die nicht den Sicherheitsstandards oder bewährten Methoden entsprechen

ARN: `arn:aws:securityhub:::insight/securityhub/default/6`

Gruppiert nach: Ressourcen-ID

Filter finden:

- Typ ist `Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices`
- Datensatzstatus ist `ACTIVE`
- Workflow-Status ist `NEW` oder `NOTIFIED`

7. AWS-Ressourcen, die mit potenziellen Datenexfiltrationen zusammenhängen

ARN: `arn:aws:securityhub:::insight/securityhub/default/7`

Gruppiert nach: Ressourcen-ID

Filter finden:

- Typ beginnt mit Effekte/Datenexfiltration/

- Datensatzstatus ist `ACTIVE`
- Workflow-Status ist `NEW` oder `NOTIFIED`

8. AWS-Ressourcen, die mit unbefugter Ressourcennutzung zusammenhängen

   ARN: `arn:aws:securityhub:::insight/securityhub/default/8`

   Gruppiert nach: Ressourcen-ID

   Filter finden:

   - Typ beginnt mit `Effects/Resource Consumption`
   - Datensatzstatus ist `ACTIVE`
   - Workflow-Status ist `NEW` oder `NOTIFIED`

9. S3-Buckets, die Sicherheitsstandards oder Best Practices nicht erfüllen

   ARN: `arn:aws:securityhub:::insight/securityhub/default/11`

   Gruppiert nach: Ressourcen-ID

   Filter finden:

   - Ressourcentyp ist `AwsS3Bucket`
   - Typ ist `Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices`
   - Datensatzstatus ist `ACTIVE`
   - Workflow-Status ist `NEW` oder `NOTIFIED`

10. S3-Buckets mit sensiblen Daten

    ARN: `arn:aws:securityhub:::insight/securityhub/default/12`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Ressourcentyp ist `AwsS3Bucket`
    - Typ beginnt mit `Sensitive Data Identifications/`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

11. Anmeldeinformationen, die möglicherweise in falsche Hände geraten sind

    ARN: `arn:aws:securityhub:::insight/securityhub/default/13`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit `Sensitive Data Identifications/Passwords/`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`
12. EC2-Instances mit fehlenden Sicherheits-Patches für wichtige Schwachstellen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/16`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit `Software and Configuration Checks/Vulnerabilities/CVE`
    - Ressourcentyp ist `AwsEc2Instance`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`
13. EC2-Instances mit allgemeinem ungewöhnlichem Verhalten

    ARN: `arn:aws:securityhub:::insight/securityhub/default/17`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit `Unusual Behaviors`
    - Ressourcentyp ist `AwsEc2Instance`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`
14. EC2-Instances, die über Ports verfügen, auf die aus dem Internet zugegriffen werden kann

    ARN: `arn:aws:securityhub:::insight/securityhub/default/18`

    Gruppiert nach: Ressourcen-ID

Filter finden:

- Typ beginnt mit `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
- Ressourcentyp ist `AwsEc2Instance`
- Datensatzstatus ist `ACTIVE`
- Workflow-Status ist `NEW` oder `NOTIFIED`

15. EC2-Instances, die Sicherheitsstandards oder Best Practices nicht erfüllen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/19`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit einer der folgenden Möglichkeiten:
      - `Software and Configuration Checks/Industry and Regulatory Standards/`
      - `Software and Configuration Checks/AWS Security Best Practices`
    - Ressourcentyp ist `AwsEc2Instance`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

16. EC2-Instances mit offenem Zugang zum Internet

    ARN: `arn:aws:securityhub:::insight/securityhub/default/21`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
    - Ressourcentyp ist `AwsEc2Instance`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

17. EC2-Instances, die mit Ausspähungen durch Widersacher zusammenhängen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/22`

Gruppiert nach: Ressourcen-ID

Filter finden:

- Typ beginnt mit TTPS/Discovery/Recon
- Ressourcentyp ist `AwsEc2Instance`
- Datensatzstatus ist `ACTIVE`
- Workflow-Status ist `NEW` oder `NOTIFIED`

18. AWS-Ressourcen, die mit Malware zusammenhängen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/23`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit einer der folgenden Möglichkeiten:
      - `Effects/Data Exfiltration/Trojan`
      - `TTPs/Initial Access/Trojan`
      - `TTPs/Command and Control/Backdoor`
      - `TTPs/Command and Control/Trojan`
      - `Software and Configuration Checks/Backdoor`
      - `Unusual Behaviors/VM/Backdoor`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

19. AWS-Ressourcen, die mit Kryptowährungsproblemen zusammenhängen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/24`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit einer der folgenden Möglichkeiten:
      - `Effects/Resource Consumption/Cryptocurrency`
      - `TTPs/Command and Control/CryptoCurrency`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

20. AWS-Ressourcen mit unbefugten Zugriffsversuchen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/25`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Typ beginnt mit einer der folgenden Möglichkeiten:
      - `TTPs/Command and Control/UnauthorizedAccess`
      - `TTPs/Initial Access/UnauthorizedAccess`
      - `Effects/Data Exfiltration/UnauthorizedAccess`
      - `Unusual Behaviors/User/UnauthorizedAccess`
      - `Effects/Resource Consumption/UnauthorizedAccess`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`
21. Bedrohungsinformationsindikatoren mit den meisten Treffern in der letzten Woche

    ARN: `arn:aws:securityhub:::insight/securityhub/default/26`

    Filter finden:

    - Erstellt innerhalb der letzten 7 Tage
22. Top-Konten nach Anzahl der Ergebnisse

    ARN: `arn:aws:securityhub:::insight/securityhub/default/27`

    Gruppiert nach: AWS-Konto ID

    Filter finden:

    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`
23. Top-Produkte nach Anzahl der Ergebnisse

    ARN: `arn:aws:securityhub:::insight/securityhub/default/28`

    Gruppiert nach: Produktname

    Filter finden:

- Datensatzstatus ist `ACTIVE`
- Workflow-Status ist `NEW` oder `NOTIFIED`

24. Schweregrad nach Anzahl der Ergebnisse

    ARN: `arn:aws:securityhub:::insight/securityhub/default/29`

    Gruppiert nach: Bezeichnung Schweregrad

    Filter finden:

    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

25. Top S3-Buckets nach Anzahl der Ergebnisse

    ARN: `arn:aws:securityhub:::insight/securityhub/default/30`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Ressourcentyp ist `AwsS3Bucket`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

26. Top-EC2-Instances nach Anzahl der Ergebnisse

    ARN: `arn:aws:securityhub:::insight/securityhub/default/31`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Ressourcentyp ist `AwsEc2Instance`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

27. Top-AMIs nach Anzahl der Ergebnisse

    ARN: `arn:aws:securityhub:::insight/securityhub/default/32`

    Gruppiert nach: Image-ID der EC2-Instanz

    Filter finden:

- Ressourcentyp ist `AwsEc2Instance`
- Datensatzstatus ist `ACTIVE`
- Workflow-Status ist `NEW` oder `NOTIFIED`

28. Top-IAM-Benutzer nach Anzahl der Ergebnisse

    ARN: `arn:aws:securityhub:::insight/securityhub/default/33`

    Gruppiert nach: IAM-Zugriffsschlüssel-ID

    Filter finden:

    - Ressourcentyp ist `AwsIamAccessKey`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

29. Top-Ressourcen nach Anzahl fehlgeschlagener CIS-Prüfungen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/34`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Generator-ID beginnt mit `arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule`
    - Aktualisiert am letzten Tag
    - Compliance-Status ist `FAILED`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

30. Top-Integrationen nach Anzahl der Ergebnisse

    ARN: `arn:aws:securityhub:::insight/securityhub/default/35`

    Gruppiert nach: Produkt ARN

    Filter finden:

    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`

31. Ressourcen mit den am meisten fehlgeschlagenen Sicherheitsprüfungen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/36`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - Aktualisiert am letzten Tag
    - Compliance-Status ist `FAILED`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`
32. IAM-Benutzer mit verdächtigen Aktivitäten

    ARN: `arn:aws:securityhub:::insight/securityhub/default/37`

    Gruppiert nach: IAM-Benutzer

    Filter finden:

    - Ressourcentyp ist `AwsIamUser`
    - Datensatzstatus ist `ACTIVE`
    - Workflow-Status ist `NEW` oder `NOTIFIED`
33. Ressourcen mit den meisten AWS Health Ergebnissen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/38`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - `ProductName`ist gleich `Health`
34. Ressourcen mit den meisten AWS Config Ergebnissen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/39`

    Gruppiert nach: Ressourcen-ID

    Filter finden:

    - `ProductName`ist gleich `Config`

35. Bewerbungen mit den meisten Ergebnissen

    ARN: `arn:aws:securityhub:::insight/securityhub/default/40`

    Gruppiert nach: ResourceApplicationArn

    Filter finden:

    - `RecordState`ist gleich `ACTIVE`
    - `Workflow.Status`ist gleich oder `NEW` `NOTIFIED`

Benutzerdefinierte Insights

Zusätzlich zu denAWSMit Security Hub verwalteten Insights können Sie benutzerdefinierte Einblicke in Security Hub erstellen, um Probleme zu verfolgen, die für Ihre Umgebung spezifisch sind. Benutzerdefinierte Einblicke bieten eine Möglichkeit, eine kuratierte Teilmenge von Problemen zu verfolgen.

Hier sind einige Beispiele für benutzerdefinierte Insights, deren Einrichtung nützlich sein kann:

- Wenn Sie ein Administratorkonto besitzen, können Sie einen benutzerdefinierten Einblick einrichten, um kritische und schwerwiegende Ergebnisse zu verfolgen, die sich auf Mitgliedskonten auswirken.
- Wenn Sie sich auf ein bestimmtes verlassenintegriertAWSBedienung, können Sie einen benutzerdefinierten Insight einrichten, um kritische und schwerwiegende Ergebnisse dieses Dienstes zu verfolgen.
- Wenn Sie sich auf eine verlassenIntegration von Drittanbieternkönnen Sie einen benutzerdefinierten Insight einrichten, um kritische und schwerwiegende Ergebnisse aus diesem integrierten Produkt zu verfolgen.

Sie können völlig neue benutzerdefinierte Insights erstellen oder von einem vorhandenen benutzerdefinierten oder verwalteten Insight ausgehen.

Jeder Insight wird mit den folgenden Optionen konfiguriert.

- Gruppierungsattribut— Das Gruppierungsattribut bestimmt, welche Elemente in der Insight-Ergebnisliste angezeigt werden. Zum Beispiel, wenn das Gruppierungsattribut lautetName des Produkts, dann zeigen die Insight-Ergebnisse die Anzahl der Ergebnisse an, die jedem Findungsanbieter zugeordnet sind.

- Optionale Filter— Die Filter grenzen die passenden Ergebnisse für den Insight ein.

  Bei der Abfrage Ihrer Ergebnisse wendet Security Hub die boolesche AND-Logik auf den Filtersatz an. Mit anderen Worten: Eine Suche stimmt nur dann überein, wenn sie mit allen bereitgestellten Filtern übereinstimmt. Wenn die Filter beispielsweise „Product name is (Produktname ist) GuardDuty" und „Resource type is (Ressourcentyp ist) `AwsS3Bucket„,lauten, müssen übereinstimmende Ergebnisse beide Kriterien erfüllen.

  Security Hub wendet jedoch die boolesche OR-Logik auf Filter an, die dasselbe Attribut, aber unterschiedliche Werte verwenden. Wenn die Filter beispielsweise lauten: „Produktname istGuardDuty„und „Der Produktname ist Amazon Inspector“, dann stimmt ein Ergebnis überein, wenn es von einem der beidenGuardDutyoder Amazon Inspector.

Beachten Sie, dass, wenn Sie die Ressourcen-ID oder den Ressourcentyp als Gruppierungsattribut verwenden, die Insight-Ergebnisse alle Ressourcen enthalten, die in den entsprechenden Ergebnissen enthalten sind. Die Liste ist nicht auf Ressourcen beschränkt, die einem Ressourcentypfilter entsprechen. Ein Insight identifiziert beispielsweise Ergebnisse, die mit S3-Buckets verknüpft sind, und gruppiert diese Ergebnisse nach Ressourcen-Identifier. Ein passendes Ergebnis enthält sowohl eine S3-Bucket-Ressource als auch eine IAM-Zugriffsschlüsselressource. Die Insight-Ergebnisse beinhalten beide Ressourcen.

Erstellen eines benutzerdefinierten Insights (Konsole)

Von der Konsole aus können Sie einen völlig neuen Insight erstellen.

Um einen benutzerdefinierten Einblick zu erstellen

1. Öffne dieAWSSecurity Hub-Konsole unterhttps://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Insights aus.
3. Wählen Sie Create Insight (Insight erstellen) aus.
4. So wählen Sie das Gruppierungsattribut für den Insight aus:

   a. Wählen Sie das Suchfeld, um die Filteroptionen anzuzeigen.

   b. Wählen Sie Group by (Gruppieren nach).

   c. Wählen Sie das Attribut aus, das verwendet werden soll, um die Ergebnisse zu gruppieren, die mit dieser Erkenntnis verknüpft sind.

   d. Wählen Sie Apply (Anwenden) aus.

5. (Optional) Wählen Sie zusätzliche Filter aus, die für diesen Insight verwendet werden sollen. Definieren Sie für jeden Filter die Filterkriterien und wählen Sie dannBewerben.
6. Wählen Sie Create Insight (Insight erstellen) aus.
7. Geben Sie einen Insight name (Insight-Name) an und wählen Sie dann Create insight (Insight erstellen) aus.

Erstellen eines benutzerdefinierten Insights (programmgesteuert)

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um programmgesteuert einen benutzerdefinierten Einblick in Security Hub zu erstellen. Sie können Filter angeben, um die Sammlung der Ergebnisse im Insight auf eine bestimmte Teilmenge einzugrenzen.

Die folgenden Tabs enthalten Anweisungen in einigen Sprachen zum Erstellen eines benutzerdefinierten Insights. Unterstützung in weiteren Sprachen finden Sie unterTools, auf denen man aufbauen kannAWS.

Security Hub API

1. Führen Sie den`CreateInsight`Betrieb.
2. Bevölkern Sie die`Name`Parameter mit einem Namen für Ihre benutzerdefinierte Einsicht.
3. Bevölkern Sie die`Filters`Parameter, um anzugeben, welche Ergebnisse in die Einsicht aufgenommen werden sollen.
4. Bevölkern Sie die`GroupByAttribute`Parameter, um anzugeben, welches Attribut verwendet wird, um die Ergebnisse zu gruppieren, die in der Erkenntnis enthalten sind.
5. Füllen Sie optional die`SortCriteria`Parameter, um die Ergebnisse nach einem bestimmten Feld zu sortieren.

   Wenn du aktiviert hastregionsübergreifende Aggregationund rufen Sie diese API von der Aggregationsregion aus auf. Die Erkenntnisse beziehen sich auf übereinstimmende Ergebnisse in der Aggregation und den verknüpften Regionen.

AWS CLI

1. Führen Sie in der Befehlszeile den`create-insight`Befehl.
2. Bevölkern Sie die`name`Parameter mit einem Namen für Ihre benutzerdefinierte Einsicht.
3. Bevölkern Sie die`filters`Parameter, um anzugeben, welche Ergebnisse in die Einsicht aufgenommen werden sollen.

4. Bevölkern Sie die`group-by-attribute`Parameter, um anzugeben, welches Attribut verwendet wird, um die Ergebnisse zu gruppieren, die in der Erkenntnis enthalten sind.

Wenn du aktiviert hastregionsübergreifende Aggregationund führen Sie diesen Befehl von der Aggregationsregion aus. Die Information bezieht sich auf übereinstimmende Ergebnisse aus der Aggregation und den verknüpften Regionen.

```
aws securityhub create-insight --name <insight name> --filters <filter values> --
group-by-attribute <attribute name>
```

Beispiel

```
aws securityhub create-insight --name "Critical role findings" --filters
 '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

1. Benutze die`New-SHUBInsight`Cmdlet.
2. Bevölkern Sie die`Name`Parameter mit einem Namen für Ihre benutzerdefinierte Einsicht.
3. Bevölkern Sie die`Filter`Parameter, um anzugeben, welche Ergebnisse in die Einsicht aufgenommen werden sollen.
4. Bevölkern Sie die`GroupByAttribute`Parameter, um anzugeben, welches Attribut verwendet wird, um die Ergebnisse zu gruppieren, die in der Erkenntnis enthalten sind.

Wenn du aktiviert hastregionsübergreifende Aggregationund verwenden Sie dieses Cmdlet aus der Aggregation Region. Die Erkenntnisse beziehen sich auf übereinstimmende Ergebnisse aus der Aggregation und den verknüpften Regionen.

Beispiel

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "XXX"
    }
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{
```

```
        Comparison = "EQUALS"
        Value = 'FAILED'
    }
}
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

Ändern eines benutzerdefinierten Insights (Konsole)

Sie können einen vorhandenen benutzerdefinierten Insight ändern, um den Gruppierungswert und die Filter zu ändern. Nachdem Sie die Änderungen vorgenommen haben, können Sie die Aktualisierungen an den ursprünglichen Insight speichern oder die aktualisierte Version als neuen Insight speichern.

Ändern eines Insight

1. Öffne dieAWSSecurity Hub-Konsole unterhttps://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Insights aus.
3. Wählen Sie den zu ändernden benutzerdefinierten Insight aus.
4. Bearbeiten Sie die Insight-Konfiguration nach Bedarf.
   - So ändern Sie das Attribut, das zum Gruppieren von Ergebnissen in dem Insight verwendet wird:
     a. Um die bestehende Gruppierung zu entfernen, wählen SieXneben demGruppieren nachEinstellung.
     b. Wählen Sie das Suchfeld aus.
     c. Wählen Sie das Attribut aus, das für die Gruppierung verwendet werden soll.
     d. Wählen Sie Apply (Anwenden) aus.
   - Um einen Filter aus der Insight zu entfernen, wählen Sie den eingekreistenXneben dem Filter.
   - So fügen Sie dem Insight einen Filter hinzu:
     a. Wählen Sie das Suchfeld aus.
     b. Wählen Sie das Attribut und den Wert aus, die als Filter verwendet werden sollen.
     c. Wählen Sie Apply (Anwenden) aus.
5. Wenn Sie die Aktualisierungen abgeschlossen haben, wählen Sie Save insight (Insight speichern).
6. Führen Sie eine der folgenden Aktionen aus, wenn Sie dazu aufgefordert werden:

- Zum Ersetzen des vorhandenen Insight durch Ihre Änderungen wählen Sie Update ***<Insight_Name>*** (<Insight_Name> aktualisieren) und dann Save insight (Insight speichern) aus.
- Um einen neuen Insight mit den Updates zu erstellen, wählen Sie Save new insight (Neuen Insight speichern. Geben Sie einen Insight name (Insight-Namen) an und wählen Sie dann Save insight (Insight speichern) aus.

Ändern eines benutzerdefinierten Insights (programmgesteuert)

Um einen benutzerdefinierten Insight zu ändern, wählen Sie Ihre bevorzugte Methode und folgen Sie den Anweisungen.

Security Hub API

1. Führen Sie den`UpdateInsight`Betrieb.
2. Um den benutzerdefinierten Insight zu identifizieren, geben Sie den Amazon-Ressourcennamen (ARN) des Insights an. Um den ARN eines benutzerdefinierten Insights abzurufen, führen Sie den`GetInsights`Betrieb.
3. Aktualisiere die`Name`,`Filters`, und`GroupByAttribute`Parameter nach Bedarf.

AWS CLI

1. Führen Sie in der Befehlszeile den`update-insight`Befehl.
2. Um den benutzerdefinierten Insight zu identifizieren, geben Sie den Amazon-Ressourcennamen (ARN) des Insights an. Um den ARN eines benutzerdefinierten Insights abzurufen, führen Sie den`get-insights`Befehl.
3. Aktualisiere die`name`,`filters`, und`group-by-attribute`Parameter nach Bedarf.

```
aws securityhub update-insight --insight-arn <insight ARN> [--name <new name>] [--
filters <new filters>] [--group-by-attribute <new grouping attribute>]
```

Beispiel

```
aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
```

```
EXAMPLE11111" --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value":
 "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --
name "High severity role findings"
```

PowerShell

1. Benutze die`Update-SHUBInsight`Cmdlet.
2. Um den benutzerdefinierten Insight zu identifizieren, geben Sie den Amazon-Ressourcennamen (ARN) des Insights an. Um den ARN eines benutzerdefinierten Insights abzurufen, verwenden Sie den`Get-SHUBInsight`Cmdlet.
3. Aktualisiere die`Name`,`Filter`, und`GroupByAttribute`Parameter nach Bedarf.

   Beispiel

```
$Filter = @{
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "AwsIamRole"
    }
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "HIGH"
    }
}

Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

Erstellen eines neuen benutzerdefinierten Insights aus einem verwalteten Insight (Konsole)

Sie können keine Änderungen an einem verwalteten Insight speichern oder löschen. Sie können einen verwalteten Insight als Grundlage für einen neuen benutzerdefinierten Insight verwenden.

So erstellen Sie einen neuen benutzerdefinierten Insight aus einem verwalteten Insight

1. Öffne dieAWSSecurity Hub-Konsole unterhttps://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Insights aus.

3. Wählen Sie die verwalteten Insights aus, von denen aus Sie arbeiten möchten.
4. Bearbeiten Sie die Insight-Konfiguration nach Bedarf.
   - So ändern Sie das Attribut, das zum Gruppieren von Ergebnissen in dem Insight verwendet wird:
     a. Um die bestehende Gruppierung zu entfernen, wählen SieXneben demGruppieren nachEinstellung.
     b. Wählen Sie das Suchfeld aus.
     c. Wählen Sie das Attribut aus, das für die Gruppierung verwendet werden soll.
     d. Wählen Sie Apply (Anwenden) aus.
   - Um einen Filter aus der Insight zu entfernen, wählen Sie den eingekreistenXneben dem Filter.
   - So fügen Sie dem Insight einen Filter hinzu:
     a. Wählen Sie das Suchfeld aus.
     b. Wählen Sie das Attribut und den Wert aus, die als Filter verwendet werden sollen.
     c. Wählen Sie Apply (Anwenden) aus.
5. Wenn Ihre Aktualisierungen abgeschlossen sind, wählen Sie Create insight (Insight erstellen).
6. Wenn Sie dazu aufgefordert werden, geben Sie einName der Einsicht, und wählen Sie dannEinblicke schaffen.

Löschen eines benutzerdefinierten Insights (Konsole)

Wenn Sie einen benutzerdefinierten Insight nicht mehr benötigen, können Sie ihn löschen. Verwaltete Insights können nicht gelöscht werden.

Löschen eines benutzerdefinierten Insight

1. Öffne dieAWSSecurity Hub-Konsole unterhttps://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Insights aus.
3. Suchen Sie den benutzerdefinierten Insight, der gelöscht werden soll.
4. Wählen Sie für diesen Einblick das Symbol „Weitere Optionen“ (die drei Punkte in der oberen rechten Ecke der Karte).
5. Wählen Sie Löschen.

Löschen eines benutzerdefinierten Insights (programmgesteuert)

Um einen benutzerdefinierten Insight zu löschen, wählen Sie Ihre bevorzugte Methode und folgen Sie den Anweisungen.

Security Hub API

1. Führen Sie den`DeleteInsight`Betrieb.
2. Um den benutzerdefinierten Insight zu identifizieren, der gelöscht werden soll, geben Sie den ARN des Insights an. Um den ARN eines benutzerdefinierten Insights abzurufen, führen Sie den`GetInsights`Betrieb.

AWS CLI

1. Führen Sie in der Befehlszeile den`delete-insight`Befehl.
2. Um den benutzerdefinierten Insight zu identifizieren, geben Sie den ARN des Insights an. Um den ARN eines benutzerdefinierten Insights abzurufen, führen Sie den`get-insights`Befehl.

```
aws securityhub delete-insight --insight-arn <insight ARN>
```

Beispiel

```
aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

PowerShell

1. Benutze die`Remove-SHUBInsight`Cmdlet.
2. Um den benutzerdefinierten Insight zu identifizieren, geben Sie den ARN des Insights an. Um den ARN eines benutzerdefinierten Insights abzurufen, verwenden Sie den`Get-SHUBInsight`Cmdlet.

Beispiel

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Automatisierungen

Mithilfe von Security Hub Hub-Automatisierungen können Sie Ergebnisse auf der Grundlage Ihrer Spezifikationen schnell ändern und korrigieren.

Security Hub unterstützt derzeit zwei Arten von Automatisierungen:

- Automatisierungsregeln — Automatische Aktualisierung und Unterdrückung von Ergebnissen nahezu in Echtzeit auf der Grundlage von von Ihnen definierter Kriterien.
- Automatisierte Reaktion und Problembehebung — Erstellen Sie benutzerdefinierte EventBridge Regeln, die automatische Maßnahmen definieren, die anhand bestimmter Ergebnisse und Erkenntnisse ergriffen werden sollen.

Automatisierungsregeln gelten vor EventBridge Regeln. Das heißt, Automatisierungsregeln werden ausgelöst und aktualisieren ein Ergebnis, bevor es an gesendet wird EventBridge. EventBridge Die Regeln gelten dann für den aktualisierten Befund.

Bei der Einrichtung von Automatisierungen für Sicherheitskontrollen empfehlen wir, nach der Kontroll-ID und nicht nach Titel oder Beschreibung zu filtern. Security Hub aktualisiert zwar gelegentlich die Titel und Beschreibungen von Steuerelementen, die Kontroll-IDs bleiben jedoch gleich.

Themen

Automation-Regeln

Automation-Regeln können verwendet werden, um Ergebnisse in Security Hub automatisch zu aktualisieren. Wenn Ergebnisse erfasst werden, kann Security Hub eine Vielzahl von Regelaktionen anwenden, z. B. das Unterdrücken von Ergebnissen, das Ändern ihres Schweregrads und das Hinzufügen von Notizen zu Ergebnissen. Solche Regelaktionen werden wirksam, wenn die Ergebnisse mit Ihren angegebenen Kriterien übereinstimmen, z. B. mit welcher Ressource oder Konto-ID die Erkenntnis verknüpft ist oder deren Titel.

Beispiele für Anwendungsfälle für Automatisierungsregeln sind:

- Erhöhen des Schweregrads einer Erkenntnis auf , `CRITICAL` wenn sich die Ressourcen-ID der Erkenntnis auf eine geschäftskritische Ressource bezieht.
- Erhöhen des Schweregrads einer Erkenntnis von `HIGH` auf , `CRITICAL` wenn sich die Erkenntnis auf Ressourcen in bestimmten Produktionskonten auswirkt.
- Zuweisen bestimmter Ergebnisse, die den Schweregrad `INFORMATIONAL` eines `SUPPRESSED` Workflow-Status aufweisen.

Automatisierungsregeln können verwendet werden, um ausgewählte Erkenntnisfelder im AWS Security Finding Format (ASFF) zu aktualisieren. Regeln gelten sowohl für neue als auch für aktualisierte Erkenntnisse.

Sie können eine benutzerdefinierte Regel von Grund auf neu erstellen oder eine von Security Hub bereitgestellte Regelvorlage verwenden. Wenn Sie eine Regelvorlage verwenden, können Sie sie nach Bedarf für Ihren Anwendungsfall ändern.

Funktionsweise von Automatisierungsregeln

Der Security Hub-Administrator kann eine Automatisierungsregel erstellen, indem er Regelkriterien definiert. Wenn ein Ergebnis den definierten Kriterien entspricht, wendet Security Hub die Regelaktion darauf an. Weitere Informationen zu verfügbaren Kriterien und Aktionen finden Sie unter Verfügbare Regelkriterien und Regelaktionen.

Nur das Security Hub-Administratorkonto kann Automatisierungsregeln erstellen, löschen, bearbeiten und anzeigen. Eine Regel, die ein Administrator erstellt, gilt für Ergebnisse im Administratorkonto und allen Mitgliedskonten. Durch die Angabe von Mitgliedskonto-IDs als Regelkriterien können Security Hub-Administratoren auch Automatisierungsregeln verwenden, um Ergebnisse zu aktualisieren oder Maßnahmen für Ergebnisse in bestimmten Mitgliedskonten zu ergreifen.

> **Important**
>
> Eine Automatisierungsregel gilt nur in der , AWS-Region in der sie erstellt wird. Um eine Regel in mehreren Regionen anzuwenden, muss der delegierte Administrator die Regel in jeder Region erstellen. Dies kann über die Security Hub-Konsole, die Security Hub-API oder erfolgenAWS CloudFormation. Sie können auch ein multiregionales Bereitstellungsskript verwenden.

Einen Verlauf darüber, wie Automatisierungsregeln Ihre Ergebnisse geändert haben, finden Sie unter Den Verlauf der Ergebnisse überprüfen.

Automatisierungsregeln gelten für neue und aktualisierte Erkenntnisse, die Security Hub generiert oder aufnimmt, nachdem Sie die Regel erstellt haben. Security Hub aktualisiert die Kontrollergebnisse alle 12–24 Stunden oder wenn die zugehörige Ressource den Status wechselt. Weitere Informationen finden Sie unterZeitplan für die Ausführung von Sicherheitsprüfungen.

Security Hub unterstützt derzeit maximal 100 Automatisierungsregeln für ein Administratorkonto.

Regelreihenfolge

Beim Erstellen von Automatisierungsregeln weisen Sie jeder Regel eine -Reihenfolge zu. Dies bestimmt die Reihenfolge, in der Security Hub Ihre Automatisierungsregeln anwendet, und wird wichtig, wenn sich mehrere Regeln auf dasselbe Erkenntnis- oder Erkenntnisfeld beziehen.

Wenn sich mehrere Regelaktionen auf dieselbe Erkenntnis oder dasselbe Erkenntnisfeld beziehen, gilt die Regel mit dem höchsten numerischen Wert für die Regelreihenfolge zuletzt und hat den endgültigen Effekt.

Wenn Sie eine Regel in der Security Hub-Konsole erstellen, weist Security Hub automatisch die Regelreihenfolge basierend auf der Reihenfolge der Regelerstellung zu. Die zuletzt erstellte Regel hat den niedrigsten numerischen Wert für die Regelreihenfolge und gilt daher zuerst. Security Hub wendet nachfolgende Regeln in aufsteigender Reihenfolge an.

Wenn Sie eine Regel über die Security Hub-API oder erstellenAWS CLI, wendet Security Hub die Regel `RuleOrder` zuerst mit dem niedrigsten numerischen Wert an. Anschließend werden nachfolgende Regeln in aufsteigender Reihenfolge angewendet. Wenn mehrere Ergebnisse denselben haben`RuleOrder`, wendet Security Hub zuerst eine Regel mit einem früheren Wert für das `UpdatedAt` Feld an (d. h. die zuletzt bearbeitete Regel gilt zuletzt).

Sie können die Regelreihenfolge jederzeit ändern.

Beispiel für die Regelreihenfolge :

Regel A (Regelreihenfolge ist **1**):

- Kriterien für Regel A
  - `ProductName` = `Security Hub`
  - `Resources.Type` ist `S3 Bucket`
  - `Compliance.Status` = `FAILED`

  - `RecordState` ist `NEW`
  - `Workflow.Status` = `ACTIVE`
- Aktionen für Regel A
  - Aktualisieren `Confidence` auf `95`
  - Aktualisieren `Severity` auf `CRITICAL`

Regel B (Regelreihenfolge ist **2**):

- Kriterien für Regel B
  - `AwsAccountId` = `123456789012`
- Aktionen für Regel B
  - Aktualisieren `Severity` auf `INFORMATIONAL`

Aktionen von Regel A gelten zuerst für Security Hub-Ergebnisse, die den Kriterien von Regel A entsprechen. Als Nächstes gelten die Aktionen von Regel B für Security Hub-Ergebnisse mit der angegebenen Konto-ID. In diesem Beispiel lautet der Endwert von `Severity` in Ergebnissen aus der angegebenen Konto-ID , da Regel B zuletzt angewendet wird`INFORMATIONAL`. Basierend auf der Aktion Regel A lautet der Endwert von `Confidence` in übereinstimmenden Ergebnissen `95`.

Verfügbare Regelkriterien und Regelaktionen

Die folgenden ASFF-Felder werden derzeit als Kriterien für Automatisierungsregeln unterstützt.

ASFF-Feld	Filter	Feldtyp
`AwsAccountId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`AwsAccountName`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Zeichenfolge

ASFF-Feld	Filter	Feldtyp
CompanyName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ComplianceAssociatedStandardsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ComplianceSecurityControlId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ComplianceStatus	Is, Is Not	Auswählen: [FAILED, NOT_AVAILABLE , PASSED, WARNING]
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Zahl
CreatedAt	Start, End, DateRange	Datum (formatiert als 2022-12-01T21:47:39.269Z)
Criticality	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Zahl
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

ASFF-Feld	Filter	Feldtyp
FirstObservedAt	Start, End, DateRange	Datum (formatiert als 2022-12-01T21:47:39.269Z)
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
LastObservedAt	Start, End, DateRange	Datum (formatiert als 2022-12-01T21:47:39.269Z)
NoteText	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
NoteUpdatedAt	Start, End, DateRange	Datum (formatiert als 2022-12-01T21:47:39.269Z)
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge

ASFF-Feld	Filter	Feldtyp
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Zuordnung

ASFF-Feld	Filter	Feldtyp
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Zuordnung
ResourceType	Is, Is Not	Auswählen (siehe Von ASFF unterstützte Ressourcen)
SeverityLabel	Is, Is Not	Auswählen: [CRITICAL, HIGH, MEDIUM, LOW, INFORMATIONAL]
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Zeichenfolge

ASFF-Feld	Filter	Feldtyp
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
UpdatedAt	Start, End, DateRange	Datum (formatiert als 2022-12-01T21:47:39.269Z)
UserDefinedFields	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Zuordnung
VerificationState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
WorkflowStatus	Is, Is Not	Auswählen: [NEW, NOTIFIED, RESOLVED, SUPPRESSED]

Die folgenden ASFF-Felder werden derzeit als Aktionen für Automatisierungsregeln unterstützt:

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

Weitere Informationen zu bestimmten ASFF-Feldern finden Sie unter AWS Security Finding Format (ASFF) Syntax und ASFF-Beispiele.

> **Tip**
>
> Wenn Security Hub keine Ergebnisse mehr für eine bestimmte Kontrolle generieren soll, empfehlen wir, die Kontrolle zu deaktivieren, anstatt eine Automatisierungsregel zu verwenden. Wenn Sie ein Steuerelement deaktivieren, stoppt Security Hub die Ausführung von Sicherheitsprüfungen und generiert keine Ergebnisse dafür, sodass Ihnen keine Gebühren für dieses Steuerelement entstehen. Wir empfehlen, Automatisierungsregeln zu verwenden, um die Werte bestimmter ASFF-Felder für Ergebnisse zu ändern, die den definierten Kriterien entsprechen. Weitere Informationen zum Deaktivieren von Kontrollen finden Sie unter Aktivierung und Deaktivierung von Steuerungen in allen Standards.

Erstellen von Automatisierungsregeln

Sie können eine benutzerdefinierte Regel von Grund auf neu erstellen oder eine vorausgefüllte Security Hub-Regelvorlage verwenden.

Sie können jeweils nur eine Automatisierungsregel erstellen. Um mehrere Automatisierungsregeln zu erstellen, befolgen Sie die Konsolenverfahren mehrmals oder rufen Sie die API oder den Befehl mehrmals mit den gewünschten Parametern auf.

Sie müssen eine Automatisierungsregel in jeder Region und jedem Konto erstellen, in dem die Regel auf Ergebnisse angewendet werden soll.

Wenn Sie eine Automatisierungsregel in der Security Hub-Konsole erstellen, zeigt Ihnen Security Hub eine Vorschau der Erkenntnisse an, für die Ihre Regel gilt. Die Vorschau wird derzeit nicht unterstützt, wenn Ihre Regelkriterien einen CONTAINS- oder NOT_CONTAINS-Filter enthalten. Sie können diese Filter für Karten- und Zeichenfolgenfeldtypen auswählen.

> **Important**
>
> AWS empfiehlt, keine personenbezogenen, vertraulichen oder sensiblen Informationen in Ihren Regelnamen, Ihre Beschreibung oder andere Felder aufzunehmen.

Erstellen einer Regel aus einer Vorlage (nur Konsole)

Derzeit unterstützt nur die Security Hub-Konsole Regelvorlagen. Diese Vorlagen spiegeln häufige Anwendungsfälle für Automatisierungsregeln wider und können Ihnen bei den ersten Schritten mit der Funktion helfen. Führen Sie die folgenden Schritte aus, um eine Automatisierungsregel aus einer Vorlage in der -Konsole zu erstellen.

Console

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich beim Security Hub-Administratorkonto an.
2. Wählen Sie im Navigationsbereich Automatisierungen aus.
3. Wählen Sie Regel erstellen aus. Wählen Sie für Regeltyp die Option Regel aus Vorlage erstellen aus.
4. Wählen Sie eine Regelvorlage aus dem Dropdown-Menü aus.
5. (Optional) Ändern Sie bei Bedarf für Ihren Anwendungsfall die Abschnitte Regel , Kriterien und Automatisierte Aktion. Sie müssen mindestens ein Regelkriterium und eine Regelaktion angeben.

   Wenn dies für die von Ihnen ausgewählten Kriterien unterstützt wird, zeigt Ihnen die Konsole eine Vorschau der Ergebnisse an, die Ihren Kriterien entsprechen.
6. Wählen Sie für Regelstatus aus, ob die Regel nach der Erstellung aktiviert oder deaktiviert werden soll.
7. (Optional) Erweitern Sie den Abschnitt Zusätzliche Einstellungen. Wählen Sie Nachfolgende Regeln ignorieren für Ergebnisse, die diesen Kriterien entsprechen aus, wenn Sie möchten, dass diese Regel die letzte Regel ist, die auf Ergebnisse angewendet wird, die den Regelkriterien entsprechen.
8. (Optional) Fügen Sie für Tags Tags als Schlüssel-Wert-Paare hinzu, damit Sie die Regel leicht identifizieren können.
9. Wählen Sie Regel erstellen aus.

Erstellen einer benutzerdefinierten Regel

Wählen Sie Ihre bevorzugte Methode aus und führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Automatisierungsregel zu erstellen.

Console

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich beim Security Hub-Administratorkonto an.
2. Wählen Sie im Navigationsbereich Automatisierungen aus.
3. Wählen Sie Regel erstellen aus. Wählen Sie für Regeltyp die Option Benutzerdefinierte Regel erstellen aus.
4. Geben Sie im Abschnitt Regel einen eindeutigen Regelnamen und eine Beschreibung für Ihre Regel ein.
5. Verwenden Sie für Kriterien die Dropdown-Menüs Schlüssel , Operator und Wert, um Ihre Regelkriterien anzugeben. Sie müssen mindestens ein Regelkriterium angeben.

   Falls für die von Ihnen ausgewählten Kriterien unterstützt, zeigt Ihnen die Konsole eine Vorschau der Ergebnisse an, die Ihren Kriterien entsprechen.
6. Verwenden Sie für Automatisierte Aktion die Dropdown-Menüs, um anzugeben, welche Erkenntnisfelder aktualisiert werden sollen, wenn die Ergebnisse Ihren Regelkriterien entsprechen. Sie müssen mindestens eine Regelaktion angeben.
7. Wählen Sie für Regelstatus aus, ob die Regel nach der Erstellung aktiviert oder deaktiviert werden soll.
8. (Optional) Erweitern Sie den Abschnitt Zusätzliche Einstellungen. Wählen Sie Nachgelagerte Regeln für Ergebnisse ignorieren aus, die diesen Kriterien entsprechen, wenn Sie möchten, dass diese Regel die letzte Regel ist, die auf Ergebnisse angewendet wird, die den Regelkriterien entsprechen.
9. (Optional) Fügen Sie für Tags Tags als Schlüssel-Wert-Paare hinzu, damit Sie die Regel leicht identifizieren können.
10. Wählen Sie Regel erstellen aus.

API

1. Führen Sie `CreateAutomationRule` über das Security Hub-Administratorkonto aus. Diese API erstellt eine Regel mit einem bestimmten Amazon-Ressourcennamen (ARN).
2. Geben Sie einen Namen und eine Beschreibung für die Regel ein.
3. Setzen Sie den `IsTerminal` Parameter auf `true`, wenn diese Regel die letzte Regel sein soll, die auf Ergebnisse angewendet wird, die den Regelkriterien entsprechen.
4. Geben Sie für den `RuleOrder` Parameter die Reihenfolge der Regel an. Security Hub wendet zuerst Regeln mit einem niedrigeren numerischen Wert für diesen Parameter an.
5. Geben Sie für den `RuleStatus` Parameter an, ob Security Hub aktivieren soll, und beginnen Sie mit der Anwendung der Regel auf Ergebnisse nach der Erstellung. Der Standardwert ist `ENABLED`, wenn kein Wert angegeben wird. Ein Wert von `DISABLED` bedeutet, dass die Regel nach der Erstellung angehalten wird.
6. Geben Sie für den `Criteria` Parameter die Kriterien an, die Security Hub zum Filtern Ihrer Ergebnisse verwenden soll. Die Regelaktion gilt für Ergebnisse, die den Kriterien entsprechen. Eine Liste der unterstützten Kriterien finden Sie unter Verfügbare Regelkriterien und Regelaktionen.
7. Geben Sie für den `Actions` Parameter die Aktionen an, die Security Hub ausführen soll, wenn eine Übereinstimmung zwischen einer Erkenntnis und Ihren definierten Kriterien besteht. Eine Liste der unterstützten Aktionen finden Sie unter Verfügbare Regelkriterien und Regelaktionen.

Beispiel für eine API-Anforderung:

```
{
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
                "Text": "Known issue that is not a risk.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }],
    "Criteria": {
```

```
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "GeneratorId": [{
            "Value": "aws-foundational-security-best-practices/v/1.0.0/IAM.1",
            "Comparison": "EQUALS"
        }]
    },
    "Description": "Sample rule description",
    "IsTerminal": false,
    "RuleName": "sample-rule-name",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
}
```

AWS CLI

1. Führen Sie den `create-automation-rule` Befehl über das Security Hub-Administratorkonto aus. Dieser Befehl erstellt eine Regel mit einem bestimmten Amazon-Ressourcennamen (ARN).
2. Geben Sie einen Namen und eine Beschreibung für die Regel ein.
3. Fügen Sie den `is-terminal` Parameter ein, wenn diese Regel die letzte Regel sein soll, die auf Ergebnisse angewendet wird, die den Regelkriterien entsprechen. Andernfalls fügen Sie den `no-is-terminal` Parameter ein.
4. Geben Sie für den `rule-order` Parameter die Reihenfolge der Regel an. Security Hub wendet zuerst Regeln mit einem niedrigeren numerischen Wert für diesen Parameter an.
5. Geben Sie für den `rule-status` Parameter an, ob Security Hub aktivieren soll, und beginnen Sie mit der Anwendung der Regel auf Ergebnisse nach der Erstellung. Der

Standardwert ist `ENABLED`, wenn kein Wert angegeben wird. Ein Wert von `DISABLED` bedeutet, dass die Regel nach der Erstellung angehalten wird.

6. Geben Sie für den `criteria` Parameter die Kriterien an, die Security Hub zum Filtern Ihrer Ergebnisse verwenden soll. Die Regelaktion gilt für Ergebnisse, die den Kriterien entsprechen. Eine Liste der unterstützten Kriterien finden Sie unter Verfügbare Regelkriterien und Regelaktionen.
7. Geben Sie für den `actions` Parameter die Aktionen an, die Security Hub ausführen soll, wenn eine Übereinstimmung zwischen einer Erkenntnis und Ihren definierten Kriterien besteht. Eine Liste der unterstützten Aktionen finden Sie unter Verfügbare Regelkriterien und Regelaktionen.

Beispielbefehl:

```
aws securityhub create-automation-rule \
--actions '[{
 "Type": "FINDING_FIELDS_UPDATE",
 "FindingFieldsUpdate": {
 "Severity": {
 "Label": "HIGH"
 },
 "Note": {
 "Text": "Known issue that is a risk. Updated by automation rules",
 "UpdatedBy": "sechub-automation"
 }
 }
 }]' \
--criteria '{
 "SeverityLabel": [{
 "Value": "INFORMATIONAL",
 "Comparison": "EQUALS"
 }]
 }' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
--region us-east-1
```

Anzeigen von Automatisierungsregeln

Wählen Sie Ihre bevorzugte Methode aus und folgen Sie den Schritten, um Ihre Automatisierungsregeln und die Details jeder Regel anzuzeigen.

Console

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich beim Security Hub-Administratorkonto an.
2. Wählen Sie im Navigationsbereich Automatisierungen aus.
3. Wählen Sie einen Regelnamen aus. Wählen Sie alternativ eine Regel aus.
4. Wählen Sie Aktionen und Anzeigen aus.

API

1. Um die Automatisierungsregeln für Ihr Konto anzuzeigen, führen `ListAutomationRules` Sie über das Security Hub-Administratorkonto aus. Diese API gibt die Regel-ARNs und andere Metadaten für Ihre Regeln zurück. Für diese API sind keine Eingabeparameter erforderlich, aber Sie können optional angeben, `MaxResults` um die Anzahl der Ergebnisse und `NextToken` als Paginierungsparameter zu begrenzen. Der Anfangswert von `NextToken` sollte sein`NULL`.

   Beispiel für eine API-Anforderung:

   ```
   {
    "MaxResults": 50,
    "NextToken": "cVpdnSampleTokenYcXgTockBW44c"
   }
   ```
2. Für weitere Regeldetails, einschließlich der Kriterien und Aktionen für eine Regel, führen Sie über das Security Hub-Administratorkonto `BatchGetAutomationRules` aus.

   Beispiel für eine API-Anforderung:

   ```
   {
       "AutomationRulesArns": [
   ```

```
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
    ]
}
```

AWS CLI

1. Um die Automatisierungsregeln für Ihr Konto anzuzeigen, führen Sie den `list-automation-rules` Befehl im Security Hub-Administratorkonto aus. Dieser Befehl gibt die Regel-ARNs und andere Metadaten für Ihre Regeln zurück. Für diesen Befehl sind keine Eingabeparameter erforderlich, aber Sie können optional angeben, `max-results` um die Anzahl der Ergebnisse und `next-token` als Paginierungsparameter zu begrenzen.

   Beispielbefehl:

   ```
   aws securityhub list-automation-rules  \
   --max-results 5 \
   --next-token cVpdnSampleTokenYcXgTockBW44c \
   --region us-east-1
   ```

2. Für weitere Regeldetails, einschließlich der Kriterien und Aktionen für eine Regel, führen Sie den `batch-get-automation-rules` Befehl im Security Hub-Administratorkonto aus.

   Beispielbefehl:

   ```
   aws securityhub batch-get-automation-rules \
   --automation-rules-arns '["arn:aws:securityhub:us-
   east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
   cdef-EXAMPLE22222"]' \
   --region us-east-1
   ```

Bearbeiten von Automatisierungsregeln

Wenn Sie eine Automatisierungsregel bearbeiten, gelten die Änderungen für neue und aktualisierte Erkenntnisse, die Security Hub nach der Bearbeitung der Regel generiert oder aufnimmt.

Wählen Sie Ihre bevorzugte Methode aus und führen Sie die Schritte aus, um den Inhalt einer Automatisierungsregel zu bearbeiten. Sie können eine oder mehrere Regeln mit einer einzigen Anforderung bearbeiten. Anweisungen zum Bearbeiten der Regelreihenfolge finden Sie unter Bearbeiten der Regelreihenfolge.

Console

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich beim Security Hub-Administratorkonto an.
2. Wählen Sie im Navigationsbereich Automatisierungen aus.
3. Wählen Sie die Regel aus, die Sie bearbeiten möchten. Wählen Sie Aktion und Bearbeiten aus.
4. Ändern Sie die Regel wie gewünscht und wählen Sie Änderungen speichern aus.

API

1. Führen Sie `BatchUpdateAutomationRules` über das Security Hub-Administratorkonto aus.
2. Geben Sie für den `RuleArn` Parameter den ARN der Regel(n) an, die Sie bearbeiten möchten.
3. Geben Sie die neuen Werte für die Parameter an, die Sie bearbeiten möchten. Sie können jeden Parameter außer bearbeiten`RuleArn`.

   Beispiel für eine API-Anforderung:

```
{
    "UpdateAutomationRulesRequestItems": [
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "RuleOrder": 15,
```

```
            "RuleStatus": "Enabled"
        },
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "RuleStatus": "Disabled"
        }
    ]
}
```

AWS CLI

1. Führen Sie den `batch-update-automation-rules` Befehl über das Security Hub-Administratorkonto aus.
2. Geben Sie für den `RuleArn` Parameter den ARN der Regel(n) an, die Sie bearbeiten möchten.
3. Geben Sie die neuen Werte für die Parameter an, die Sie bearbeiten möchten. Sie können jeden Parameter außer bearbeiten`RuleArn`.

Beispielbefehl:

```
aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
    {
      "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
          "Note": {
            "Text": "Known issue that is a risk",
            "UpdatedBy": "sechub-automation"
          },
          "Workflow": {
            "Status": "NEW"
          }
        }
      }],
      "Criteria": {
        "SeverityLabel": [{
         "Value": "LOW",
         "Comparison": "EQUALS"
        }]
```

```
      },
      "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RuleOrder": 14,
      "RuleStatus": "DISABLED",
    }
  ]' \
--region us-east-1
```

Bearbeiten der Regelreihenfolge

In einigen Fällen möchten Sie möglicherweise die Regelkriterien und -aktionen unverändert lassen, aber die Reihenfolge ändern, in der Security Hub eine Automatisierungsregel anwendet. Wählen Sie Ihre bevorzugte Methode aus und folgen Sie den Schritten zum Bearbeiten der Regelreihenfolge.

Console

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich beim Security Hub-Administratorkonto an.
2. Wählen Sie im Navigationsbereich Automatisierungen aus.
3. Wählen Sie die Regel aus, deren Reihenfolge Sie ändern möchten. Wählen Sie Priorität bearbeiten aus.
4. Wählen Sie Nach oben verschieben, um die Priorität der Regel um eine Einheit zu erhöhen. Wählen Sie Nach unten verschieben, um die Priorität der Regel um eine Einheit zu verringern. Wählen Sie Nach oben verschieben, um der Regel eine Reihenfolge von 1 zuzuweisen (dies gibt der Regel Vorrang vor anderen vorhandenen Regeln).

> **Note**
>
> Wenn Sie eine Regel in der Security Hub-Konsole erstellen, weist Security Hub automatisch die Regelreihenfolge basierend auf der Reihenfolge der Regelerstellung zu. Die zuletzt erstellte Regel hat den niedrigsten numerischen Wert für die Regelreihenfolge und gilt daher zuerst.

API

1. Führen Sie `BatchUpdateAutomationRules` über das Security Hub-Administratorkonto aus.
2. Geben Sie für den `RuleArn` Parameter den ARN der Regel(n) an, deren Reihenfolge Sie bearbeiten möchten.
3. Ändern Sie den Wert des `RuleOrder` Felds.

> **Note**
>
> Wenn mehrere Regeln denselben haben`RuleOrder`, wendet Security Hub zuerst eine Regel mit einem früheren Wert für das `UpdatedAt` Feld an (d. h. die zuletzt bearbeitete Regel gilt zuletzt).

AWS CLI

1. Führen Sie den `batch-update-automation-rules` Befehl über das Security Hub-Administratorkonto aus.
2. Geben Sie für den `RuleArn` Parameter den ARN der Regel(n) an, deren Reihenfolge Sie bearbeiten möchten.
3. Ändern Sie den Wert des `RuleOrder` Felds.

> **Note**
>
> Wenn mehrere Regeln denselben haben`RuleOrder`, wendet Security Hub zuerst eine Regel mit einem früheren Wert für das `UpdatedAt` Feld an (d. h. die zuletzt bearbeitete Regel gilt zuletzt).

Löschen von Automatisierungsregeln

Wenn Sie eine Automatisierungsregel löschen, entfernt Security Hub sie aus Ihrem Konto und wendet die Regel nicht mehr auf Ergebnisse an.

Wählen Sie Ihre bevorzugte Methode aus und folgen Sie den Schritten zum Löschen einer Automatisierungsregel. Sie können eine oder mehrere Regeln in einer einzigen Anforderung löschen.

> **Tip**
>
> Alternativ zum Löschen können Sie eine Regel deaktivieren. Dadurch wird die Regel für die zukünftige Verwendung beibehalten, aber Security Hub wendet die Regel erst auf übereinstimmende Erkenntnisse an, wenn Sie sie aktivieren.

Console

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich beim Security Hub-Administratorkonto an.
2. Wählen Sie im Navigationsbereich Automatisierungen aus.
3. Wählen Sie die Regel(n) aus, die Sie löschen möchten. Wählen Sie Aktion und Löschen (um eine Regel beizubehalten, sie aber vorübergehend zu deaktivieren, wählen Sie Deaktivieren).
4. Bestätigen Sie Ihre Wahl und wählen Sie Delete (Löschen) aus.

API

1. Führen Sie `BatchDeleteAutomationRules` über das Security Hub-Administratorkonto aus.
2. Geben Sie für den `-AutomationRulesArns`Parameter den ARN der Regel(en) an, die Sie löschen möchten (um eine Regel beizubehalten, aber vorübergehend zu deaktivieren, geben Sie `DISABLED` für den `-RuleStatus`Parameter an).

   Beispiel für eine API-Anforderung:

```
{
    "AutomationRulesArns": [
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
```

```
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
    ]
}
```

AWS CLI

1. Führen Sie den `batch-delete-automation-rules` Befehl über das Security Hub-Administratorkonto aus.
2. Geben Sie für den `automation-rules-arns` Parameter den ARN der Regel(en) an, die Sie löschen möchten (um eine Regel beizubehalten, aber vorübergehend zu deaktivieren, geben Sie `DISABLED` für den `RuleStatus` Parameter an).

Beispielbefehl:

```
aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"]' \
--region us-east-1
```

Beispiele für Automatisierungsregeln

Dieser Abschnitt enthält einige Beispiele für Automatisierungsregeln für häufige Anwendungsfälle. Diese Beispiele entsprechen Regelvorlagen in der Security Hub-Konsole.

Erhöhen des Schweregrads auf Kritisch, wenn eine bestimmte Ressource, z. B. ein S3-Bucket, gefährdet ist

In diesem Beispiel werden die Regelkriterien erfüllt, wenn der `ResourceId` in einer Erkenntnis ein bestimmter Amazon Simple Storage Service (Amazon S3)-Bucket ist. Die Regelaktion besteht darin, den Schweregrad übereinstimmender Ergebnisse in zu ändern`CRITICAL`. Sie können diese Vorlage so ändern, dass sie auf andere Ressourcen angewendet wird.

Beispiel für eine API-Anforderung:

```
{
```

```
    "IsTerminal": true,
    "RuleName": "Elevate severity of findings that relate to important resources",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity to CRITICAL when specific resource such as
 an S3 bucket is at risk",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "ResourceId": [{
            "Value": "arn:aws:s3:::examplebucket/developers/design_info.doc",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "This is a critical resource. Please review ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Beispiel-CLI-Befehl:

```
aws securityhub create-automation-rule \
--is-terminal \
--rule-name "Elevate severity of findings that relate to important resources" \
--rule-order 1 \
--rule-status "ENABLED" \

--description "Elevate finding severity to CRITICAL when specific resource such as an
 S3 bucket is at risk" \
--criteria '{
"ProductName": [{
"Value": "Security Hub",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"ResourceId": [{
"Value": "arn:aws:s3:::examplebucket/developers/design_info.doc",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "This is a critical resource. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
```

```
--region us-east-1
```

Schweregrad der Erkenntnisse, die sich auf Ressourcen in Produktionskonten beziehen

In diesem Beispiel werden die Regelkriterien erfüllt, wenn in bestimmten Produktionskonten ein `HIGH` Schweregradergebnis generiert wird. Die Regelaktion besteht darin, den Schweregrad übereinstimmender Ergebnisse in zu ändern`CRITICAL`.

Beispiel für eine API-Anforderung:

```
{
    "IsTerminal": false,
    "RuleName": "Elevate severity for production accounts",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity from HIGH to CRITICAL for findings that
 relate to resources in specific production accounts",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "HIGH",
            "Comparison": "EQUALS"
        }],
        "AwsAccountId": [
        {
            "Value": "111122223333",
            "Comparison": "EQUALS"
```

```
        },
        {
            "Value": "123456789012",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "A resource in production accounts is at risk. Please review
 ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Beispiel-CLI-Befehl :

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Elevate severity of findings that relate to resources in production
 accounts" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate
 to resources in specific production accounts" \
--criteria '{
"ProductName": [{
"Value": "Security Hub",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
```

```
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "HIGH",
"Comparison": "EQUALS"
}],
"AwsAccountId": [
{
"Value": "111122223333",
"Comparison": "EQUALS"
},
{
"Value": "123456789012",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "A resource in production accounts is at risk. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Unterdrücken von Informationsergebnissen

In diesem Beispiel werden die Regelkriterien für `INFORMATIONAL` Schweregraderkenntnisse abgeglichen, die von Amazon an Security Hub gesendet werden GuardDuty. Die Regelaktion besteht darin, den Workflow-Status übereinstimmender Ergebnisse in zu ändern`SUPPRESSED`.

Beispiel für eine API-Anforderung:

```
{
    "IsTerminal": false,
    "RuleName": "Suppress informational findings",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
```

```
    "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
    "Criteria": {
        "ProductName": [{
            "Value": "GuardDuty",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "INFORMATIONAL",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
                "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL
 severity",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Beispiel-CLI-Befehl :

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
```

```
--criteria '{
"ProductName": [{
"Value": "GuardDuty",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "INFORMATIONAL",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Workflow": {
"Status": "SUPPRESSED"
},
"Note": {
"Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Automatisierte Reaktion und Problembehebung

Mit Amazon können Sie Ihre AWS Services so automatisieren EventBridge, dass sie automatisch auf Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen reagieren. Ereignisse im AWS Rahmen von Services werden nahezu EventBridge in Echtzeit und auf garantierter Basis bereitgestellt. Sie können einfache Regeln schreiben, um anzugeben, an welchen

Ereignissen Sie interessiert sind und welche automatisierten Aktionen ergriffen werden sollen, wenn ein Ereignis einer Regel entspricht. Die folgenden Aktionen können beispielsweise automatisch ausgelöst werden:

- Aufrufen einer AWS Lambda-Funktion
- Aufrufen des Amazon EC2 EC2-Run-Befehls
- Weiterleiten des Ereignisses an Amazon Kinesis Data Streams
- Aktivieren eines AWS Step Functions-Zustandsautomaten
- Benachrichtigen eines Amazon SNS-Themas oder einer Amazon SQS-Warteschlange
- Senden eines Funds an ein Ticketing-, Chat-, SIEM- oder Incident-Response- und Management-Tool eines Drittanbieters

Security Hub sendet automatisch alle neuen Ergebnisse und alle Aktualisierungen vorhandener Ergebnisse EventBridge als EventBridge Ereignisse an. Sie können auch benutzerdefinierte Aktionen erstellen, mit denen Sie ausgewählte Ergebnisse und Insight-Ergebnisse an senden können EventBridge.

Anschließend konfigurieren Sie EventBridge Regeln, um auf jeden Ereignistyp zu reagieren.

Weitere Informationen zur Verwendung EventBridge finden Sie im EventBridge Amazon-Benutzerhandbuch.

> **Note**
>
> Als bewährte Methode sollten Sie sicherstellen, dass für die Zugriffsberechtigungen, die Ihren Benutzern gewährt werden, IAM-Richtlinien mit den geringsten Rechten EventBridge verwendet werden, die nur die erforderlichen Berechtigungen gewähren.
> Weitere Informationen finden Sie unter Identitäts- und Zugriffsverwaltung in Amazon EventBridge.

Eine Reihe von Vorlagen für kontenübergreifende automatisierte Reaktionen und Problembehebungen ist auch unter Lösungen verfügbar. AWS Die Vorlagen nutzen EventBridge Ereignisregeln und Lambda-Funktionen. Sie stellen die Lösung mit AWS CloudFormation und AWS Systems Manager bereit. Die Lösung kann vollautomatische Reaktions- und Abhilfemaßnahmen erstellen. Es kann auch benutzerdefinierte Security Hub Hub-Aktionen verwenden, um vom Benutzer

ausgelöste Reaktions- und Abhilfemaßnahmen zu erstellen. Einzelheiten zur Konfiguration und Verwendung der Lösung finden Sie auf der Lösungsseite Automated Security Response. AWS

Themen

Arten der Security Hub Hub-Integration mit EventBridge

Security Hub verwendet die folgenden EventBridge Ereignistypen, um die folgenden Arten der Integration mit zu unterstützen EventBridge.

Auf dem EventBridge Dashboard für Security Hub umfasst Alle Ereignisse all diese Ereignistypen.

Alle Funde (Security Hub Findings - Imported)

Security Hub sendet automatisch alle neuen Ergebnisse und alle Aktualisierungen vorhandener Ergebnisse EventBridge als Security Hub Findings - ImportedEreignisse an. Jedes Security Hub Findings - ImportedEreignis enthält ein einzelnes Ergebnis.

Jede `BatchImportFindings`AND-Anfrage `BatchUpdateFindings` löst ein Security Hub Findings - ImportedEreignis aus.

Bei Administratorkonten EventBridge enthält der Event-Feed Ereignisse für Ergebnisse sowohl aus ihrem Konto als auch aus ihren Mitgliedskonten.

In einer Aggregationsregion enthält der Event-Feed Ereignisse für Ergebnisse aus der Aggregationsregion und den verknüpften Regionen. Regionsübergreifende Ergebnisse werden nahezu in Echtzeit in den Event-Feed aufgenommen. Informationen zur Konfiguration der Suchaggregation finden Sie unter. Regionsübergreifende Aggregation

Sie können Regeln definieren EventBridge , die Ergebnisse automatisch an einen Amazon S3 S3-Bucket, einen Korrektur-Workflow oder ein Drittanbieter-Tool weiterleiten. Die Regeln können Filter enthalten, die die Regel nur anwenden, wenn das Ergebnis bestimmte Attributwerte enthält.

Sie verwenden diese Methode, um automatisch alle Ergebnisse oder alle Ergebnisse, die bestimmte Merkmale aufweisen, an einen Reaktions- oder Behebungsworkflow zu senden.

Siehe the section called “Konfiguration einer Regel für automatisch gesendete Ergebnisse”.

Funde für benutzerdefinierte Aktionen (Security Hub Findings - Custom Action)

Security Hub sendet auch Ergebnisse, die mit benutzerdefinierten Aktionen verknüpft sind, EventBridge als Security Hub Findings - Custom ActionEreignisse an.

Dies ist nützlich für Analysten, die mit der Security Hub Hub-Konsole arbeiten und ein bestimmtes Ergebnis oder eine kleine Gruppe von Ergebnissen an einen Reaktions- oder Behebungsworkflow senden möchten. Sie können eine benutzerdefinierte Aktion für bis zu 20 Funde gleichzeitig auswählen. Jedes Ergebnis wird EventBridge als separates EventBridge Ereignis gesendet.

Wenn Sie eine benutzerdefinierte Aktion erstellen, weisen Sie ihr eine benutzerdefinierte Aktions-ID zu. Sie können diese ID verwenden, um eine EventBridge Regel zu erstellen, die eine bestimmte Aktion ausführt, nachdem sie ein Ergebnis erhalten hat, das mit dieser benutzerdefinierten Aktions-ID verknüpft ist.

Siehe the section called “Konfiguration und Verwendung benutzerdefinierter Aktionen”.

Sie können beispielsweise eine benutzerdefinierte Aktion in Security Hub mit dem Namen erstellen`send_to_ticketing`. Anschließend erstellen Sie eine Regel EventBridge, die ausgelöst wird, wenn ein Ergebnis EventBridge eingeht, das die `send_to_ticketing` benutzerdefinierte Aktions-ID enthält. Die Regel beinhaltet eine Logik zum Senden der Funde an Ihr Ticketing-System. Sie können dann Ergebnisse in Security Hub auswählen und die benutzerdefinierte Aktion in Security Hub verwenden, um Ergebnisse manuell an Ihr Ticketsystem zu senden.

Beispiele dafür, wie Sie Security Hub Hub-Ergebnisse EventBridge zur weiteren Verarbeitung an diese senden können, finden Sie im Blog How to Integrate AWS Security Hub Custom Actions with PagerDuty and How to Enable Custom Actions in AWS Security Hub on the AWS Partner Network (APN) -Blog.

Insight-Ergebnisse für benutzerdefinierte Aktionen (Security Hub Insight Results)

Sie können auch benutzerdefinierte Aktionen verwenden, um Gruppen von Insight-Ergebnissen EventBridge als Security Hub Insight ResultsEreignisse zu senden. Insight-Ergebnisse sind die Ressourcen, die einem Einblick entsprechen. Beachten Sie, dass Sie, wenn Sie Insight-

Ergebnisse an senden EventBridge, die Ergebnisse nicht an diese senden EventBridge. Sie senden nur die Ressourcen-IDs, die mit den Insight-Ergebnissen verknüpft sind. Sie können bis zu 100 Ressourcenkennungen gleichzeitig senden.

Ähnlich wie bei benutzerdefinierten Aktionen für Ergebnisse erstellen Sie zuerst die benutzerdefinierte Aktion in Security Hub und dann eine Regel in EventBridge.

Siehe the section called “Konfiguration und Verwendung benutzerdefinierter Aktionen”.

Angenommen, Sie sehen ein bestimmtes Insight-Ergebnis von Interesse, das Sie mit einem Kollegen teilen möchten. In diesem Fall können Sie eine benutzerdefinierte Aktion verwenden, um dieses Insight-Ergebnis über ein Chat- oder Ticketsystem an den Kollegen zu senden.

EventBridge Veranstaltungsformate für Security Hub

Die Security Hub Insight ResultsEreignistypen Security Hub Findings - ImportedSecurity Findings - Custom Action, und verwenden die folgenden Ereignistypen.

Das Ereignisformat ist das Format, das verwendet wird, wenn Security Hub ein Ereignis an sendet EventBridge.

Security Hub Findings - Imported

Security Hub Findings - ImportedEreignisse, die von Security Hub gesendet werden, um das folgende Format zu EventBridge verwenden.

```
{
   "version":"0",
   "id":"CWE-event-id",
   "detail-type":"Security Hub Findings - Imported",
   "source":"aws.securityhub",
   "account":"111122223333",
   "time":"2019-04-11T21:52:17Z",
   "region":"us-west-2",
   "resources":[
      "arn:aws:securityhub:us-west-2::product/aws/macie/arn:aws:macie:us-
west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/
f2893b211841"
   ],
   "detail":{
      "findings": [{
```

```
          <finding content>
        }]
    }
}
```

*<finding content>*ist der Inhalt des Ergebnisses, das durch das Ereignis gesendet wird, im JSON-Format. Jedes Ereignis sendet einen einzelnen Befund.

Eine vollständige Liste der Suchattribute finden Sie unterAWS Format für Sicherheitssuche (ASFF).

Informationen zur Konfiguration von EventBridge Regeln, die durch diese Ereignisse ausgelöst werden, finden Sie unterthe section called “Konfiguration einer Regel für automatisch gesendete Ergebnisse”.

Security Hub Findings - Custom Action

Security Hub Findings - Custom ActionEreignisse, die von Security Hub gesendet werden, um das folgende Format zu EventBridge verwenden. Jedes Ergebnis wird in einem separaten Ereignis gesendet.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Findings - Custom Action",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
  ],
  "detail": {
    "actionName":"custom-action-name",
    "actionDescription": "description of the action",
    "findings": [
      {
        <finding content>
      }
    ]
  }
}
```

*<finding content>*ist der Inhalt des Ergebnisses, das durch das Ereignis gesendet wird, im JSON-Format. Jedes Ereignis sendet einen einzelnen Befund.

Eine vollständige Liste der Suchattribute finden Sie unterAWS Format für Sicherheitssuche (ASFF).

Informationen zur Konfiguration von EventBridge Regeln, die durch diese Ereignisse ausgelöst werden, finden Sie unterthe section called “Konfiguration und Verwendung benutzerdefinierter Aktionen”.

Security Hub Insight Results

Security Hub Insight ResultsEreignisse, die von Security Hub gesendet werden, um das folgende Format zu EventBridge verwenden.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Insight Results",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
      "arn:aws:securityhub:us-west-1:111122223333::product/aws/macie:us-
west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
  ],
  "detail": {
    "actionName":"name of the action",
    "actionDescription":"description of the action",
    "insightArn":"ARN of the insight",
    "insightName":"Name of the insight",
    "resultType":"ResourceAwsIamAccessKeyUserName",
    "number of results":"number of results, max of 100",
    "insightResults": [
        {"result 1": 5},
        {"result 2": 6}
    ]
  }
}
```

Informationen zum Erstellen einer EventBridge Regel, die durch diese Ereignisse ausgelöst wird, finden Sie unterthe section called “Konfiguration und Verwendung benutzerdefinierter Aktionen”.

Konfiguration einer EventBridge Regel für automatisch gesendete Ergebnisse

Sie können eine Regel erstellen EventBridge , die eine Aktion definiert, die ausgeführt werden soll, wenn ein Security Hub Findings - ImportedEreignis empfangen wird. Security Hub Findings - ImportedEreignisse werden durch Aktualisierungen sowohl von als `BatchImportFindings`auch ausgelöst `BatchUpdateFindings`.

Jede Regel enthält ein Ereignismuster, das die Ereignisse identifiziert, die die Regel auslösen. Das Ereignismuster enthält immer die Ereignisquelle (`aws.securityhub`) und den Ereignistyp (Security Hub Hub-Ergebnisse — Importiert). Das Ereignismuster kann auch Filter angeben, um die Ergebnisse zu identifizieren, für die die Regel gilt.

Die Regel identifiziert dann die Regelziele. Die Ziele sind die Aktionen, die ergriffen werden müssen, EventBridge wenn ein Ereignis aus Security Hub Findings — Imported eingeht und das Ergebnis den Filtern entspricht.

Die hier bereitgestellten Anweisungen verwenden die EventBridge Konsole. Wenn Sie die Konsole verwenden, EventBridge wird automatisch die erforderliche ressourcenbasierte Richtlinie erstellt, die das Schreiben EventBridge in Protokolle ermöglicht. CloudWatch

Sie können auch den `PutRule`API-Betrieb der EventBridge API verwenden. Wenn Sie jedoch die EventBridge API verwenden, müssen Sie die ressourcenbasierte Richtlinie erstellen. Einzelheiten zu den erforderlichen Richtlinien finden Sie unter CloudWatch Logs-Berechtigungen im EventBridge Amazon-Benutzerhandbuch.

Format des Ereignismusters

Das Format des Ereignismusters für Security Hub Findings — Importierte Ereignisse lautet wie folgt:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
```

```
  }
}
```

- `source`identifiziert Security Hub als den Dienst, der das Ereignis generiert.
- `detail-type`identifiziert den Ereignistyp.
- `detail`ist optional und stellt die Filterwerte für das Ereignismuster bereit. Wenn das Ereignismuster kein `detail` Feld enthält, lösen alle Ergebnisse die Regel aus.

Sie können die Ergebnisse auf der Grundlage eines beliebigen Ergebnisattributs filtern. Für jedes Attribut geben Sie ein durch Kommas getrenntes Array mit einem oder mehreren Werten an.

```
"<attribute name>": [ "<value1>", "<value2>"]
```

Wenn Sie mehr als einen Wert für ein Attribut angeben, werden diese Werte durch verknüpft. `OR` Ein Ergebnis entspricht dem Filter für ein einzelnes Attribut, wenn das Ergebnis einen der aufgelisteten Werte enthält. Wenn Sie beispielsweise `INFORMATIONAL` sowohl als auch `LOW` als Werte für angeben`Severity.Label`, stimmt das Ergebnis überein, wenn es den Schweregrad entweder `INFORMATIONAL` oder hat`LOW`.

Die Attribute werden durch verknüpft`AND`. Ein Ergebnis stimmt überein, wenn es den Filterkriterien für alle angegebenen Attribute entspricht.

Wenn Sie einen Attributwert angeben, muss dieser die Position dieses Attributs innerhalb der ASFF-Struktur (AWSSecurity Finding Format) widerspiegeln.

> **Tip**
>
> Wir empfehlen, beim Filtern von Kontrollergebnissen die [Felder `SecurityControlId` oder `SecurityControlArn` ASFF] als Filter zu verwenden und nicht oder. `Title` `Description` Letztere Felder können sich gelegentlich ändern, wohingegen die Kontroll-ID und der ARN statische Identifikatoren sind.

Im folgenden Beispiel stellt das Ereignismuster Filterwerte für `ProductArn` und bereit`Severity.Label`, sodass ein Ergebnis zutrifft, wenn es von Amazon Inspector generiert wurde und den Schweregrad entweder `INFORMATIONAL` oder hat`LOW`.

```
{
```

```
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Security Hub Findings - Imported"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
    }
}
```

Eine Ereignisregel erstellen

Sie können ein vordefiniertes oder ein benutzerdefiniertes Ereignismuster verwenden, um eine Regel in zu erstellen EventBridge. Wenn Sie ein vordefiniertes Muster auswählen, EventBridge wird automatisch `source` und ausgefülltdetail-type. EventBridge stellt außerdem Felder zur Angabe von Filterwerten für die folgenden Suchattribute bereit:

- `AwsAccountId`
- `Compliance.Status`
- `Criticality`
- `ProductArn`
- `RecordState`
- `ResourceId`
- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

Um eine EventBridge Regel zu erstellen

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.

2. Erstellen Sie mit den folgenden Werten eine EventBridge Regel, die das Auffinden von Ereignissen überwacht:

   - Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.
   - Wählen Sie aus, wie das Ereignismuster erstellt werden soll.

Um das Ereignismuster zu erstellen mit...	Vorgehensweise	
Eine Vorlage	Wählen Sie im Abschnitt Ereignismuster die folgenden Optionen aus: • Als Event source (Ereignisquelle) wählen Sie AWS-Services aus. • Wählen Sie als AWSService Security Hub. • Wählen Sie als Ereignist yp die Option Security Hub Findings — Importier t aus. • (Optional) Fügen Sie Filterwerte hinzu, um die Regel spezifischer zu gestalten. Um die Regel beispielsweise auf Ergebnisse mit aktivem Datensatzstatus zu beschränken, wählen Sie für Spezifische Datensatz status die Option Aktiv aus.	

Um das Ereignismuster zu erstellen mit...	Vorgehensweise	
Ein benutzerdefiniertes Ereignismuster (Verwenden Sie ein benutzerdefiniertes Muster, wenn Sie Ergebnisse anhand von Attributen filtern möchten, die nicht in der EventBridge Konsole angezeigt werden.)	• Wählen Sie im Abschnitt Ereignismuster die Option Benutzerdefinierte Muster (JSON-Editor) aus, und fügen Sie dann das folgende Ereignismuster in den Textbereich ein: `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "<attribute name>": [ "<value1>", "<value2>"] } } }` • Aktualisieren Sie das Ereignismuster so, dass es die Attribut- und Attributwerte enthält, die Sie als Filter verwenden möchten. Verwenden Sie beispielsweise das folgende	

Um das Ereignismuster zu erstellen mit...	Vorgehensweise	
	Musterbeispiel, um die Regel auf Ergebnisse anzuwenden`TRUE_POSITIVE` , die den Bestätigungsstatus haben: `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "VerificationState": ["TRUE_POSITIVE"] } } }`	

- Für Target types (Zieltypen), wählen Sie AWS-Service, und für Select a target (Ziel auswählen), wählen Sie ein Ziel wie ein Amazon-SNS-Thema oder eine AWS Lambda-Funktion. Das Ziel wird ausgelöst, wenn ein Ereignis empfangen wird, das dem in der Regel definierten Ereignismuster entspricht.

Einzelheiten zum Erstellen von Regeln finden Sie im EventBridge Amazon-Benutzerhandbuch unter Erstellen von EventBridge Amazon-Regeln, die auf Ereignisse reagieren.

Verwenden von benutzerdefinierten Aktionen zum Senden von Ergebnissen und Erkenntnisergebnissen an EventBridge

Um benutzerdefinierte Security Hub-Aktionen zum Senden von Ergebnissen oder Insight-Ergebnissen zu verwenden EventBridge, erstellen Sie zunächst die benutzerdefinierte Aktion in Security Hub. Definieren Sie anschließend Regeln EventBridge , die für Ihre benutzerdefinierten Aktionen gelten.

Sie können bis zu 50 benutzerdefinierte Aktionen erstellen.

Wenn Sie die regionsübergreifende Aggregation aktiviert haben und Ergebnisse aus der Aggregationsregion verwalten, erstellen Sie benutzerdefinierte Aktionen in der Aggregationsregion.

Die Regel EventBridge verwendet den ARN aus der benutzerdefinierten Aktion.

Eine benutzerdefinierte Aktion erstellen (Konsole)

Wenn Sie eine benutzerdefinierte Aktion erstellen, geben Sie den Namen, die Beschreibung und eine eindeutige Kennung an.

Um eine benutzerdefinierte Aktion in Security Hub (Konsole) zu erstellen

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) und dann Custom actions (Benutzerdefinierte Aktionen) aus.
3. Wählen Sie Create custom action (Benutzerdefinierte Aktion erstellen) aus.
4. Machen Sie für die Aktion Angaben bei Name, Description (Beschreibung) und Custom action ID (Benutzerdefinierte Aktions-ID).

   Der Name muss weniger als 20 Zeichen lang sein.

   Die benutzerdefinierte Aktions-ID muss für jedes AWS Konto eindeutig sein.
5. Wählen Sie Create custom action (Benutzerdefinierte Aktion erstellen) aus.
6. Notieren Sie sich den Custom action ARN (Benutzerdefinierter Aktions-ARN). Sie müssen den ARN verwenden, wenn Sie eine Regel erstellen, um sie in EventBridge dieser Aktion zuzuordnen.

Eine benutzerdefinierte Aktion erstellen (Security Hub Hub-API,AWS CLI)

Um eine benutzerdefinierte Aktion zu erstellen, können Sie einen API-Aufruf oder den verwendenAWS Command Line Interface.

Um eine benutzerdefinierte Aktion zu erstellen (Security Hub Hub-API,AWS CLI)

- Security Hub Hub-API — Verwenden Sie den `CreateActionTarget`Vorgang. Wenn Sie eine benutzerdefinierte Aktion erstellen, geben Sie den Namen, die Beschreibung und die benutzerdefinierte Aktions-ID an.
- AWS CLI— Führen Sie den Befehl in der `create-action-target`Befehlszeile aus.

```
create-action-target --name <customActionName> --
description <customActionDescription> --id <customActionidentifier>
```

Beispiel

```
aws securityhub create-action-target --name "Send to remediation" --description
 "Action to send the finding for remediation tracking" --id "Remediation"
```

Definition einer Regel in EventBridge

Um die benutzerdefinierte Aktion zu verarbeiten, müssen Sie eine entsprechende Regel in erstellen EventBridge. Die Regeldefinition beinhaltet den ARN der benutzerdefinierten Aktion.

Das Ereignismuster für ein Security Hub Findings — Custom Action-Ereignis hat das folgende Format:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Das Ereignismuster für ein Security Hub Insight Results-Ereignis hat das folgende Format:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

In beiden Mustern *<custom action ARN>* ist dies der ARN einer benutzerdefinierten Aktion. Sie können eine Regel konfigurieren, die für mehr als eine benutzerdefinierte Aktion gilt.

Die hier bereitgestellten Anweisungen gelten für die EventBridge Konsole. Wenn Sie die Konsole verwenden, EventBridge wird automatisch die erforderliche ressourcenbasierte Richtlinie erstellt, die das Schreiben EventBridge in Protokolle ermöglicht. CloudWatch

Sie können auch den `PutRule`API-Betrieb der EventBridge API verwenden. Wenn Sie jedoch die EventBridge API verwenden, müssen Sie die ressourcenbasierte Richtlinie erstellen. Einzelheiten zu den erforderlichen Richtlinien finden Sie unter CloudWatch Logs-Berechtigungen im EventBridge Amazon-Benutzerhandbuch.

Um eine Regel zu definieren in EventBridge

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Rules aus.
3. Wählen Sie Regel erstellen.
4. Geben Sie einen Namen und eine Beschreibung für die Regel ein.
5. Wählen Sie für Event Bus den Event Bus aus, den Sie dieser Regel zuordnen möchten. Wenn Sie möchten, dass diese Regel mit Ereignissen aus Ihrem eigenen Konto übereinstimmt, wählen Sie Standard aus. Wenn ein AWS-Service in Ihrem Konto ein Ereignis ausgibt, wird es stets an den Standard-Event-Bus Ihres Kontos weitergeleitet.
6. Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.
7. Wählen Sie Weiter.
8. Wählen Sie unter Event source (Ereignisquelle) AWS events (Ereignisse) aus.
9. Wählen Sie für Ereignismuster die Option Ereignismusterformular.

10. Als Event source (Ereignisquelle) wählen Sie AWS-Services aus.
11. Wählen Sie als AWSService Security Hub.
12. Führen Sie für Type (Typ) eine der folgenden Aktionen aus:

    - Um eine Regel zu erstellen, die angewendet wird, wenn Sie Ergebnisse an eine benutzerdefinierte Aktion senden, wählen Sie Security Hub Hub-Ergebnisse — Benutzerdefinierte Aktion.
    - Um eine Regel zu erstellen, die angewendet wird, wenn Sie Insight-Ergebnisse an eine benutzerdefinierte Aktion senden, wählen Sie Security Hub Insight-Ergebnisse.
13. Wählen Sie Spezifische benutzerdefinierte Aktions-ARNs und fügen Sie einen benutzerdefinierten Aktions-ARN hinzu.

    Wenn die Regel für mehrere benutzerdefinierte Aktionen gilt, wählen Sie Hinzufügen aus, um weitere ARNs für benutzerdefinierte Aktionen hinzuzufügen.
14. Wählen Sie Weiter.
15. Wählen und konfigurieren Sie unter Ziele auswählen das Ziel, das aufgerufen werden soll, wenn diese Regel erfüllt ist.
16. Wählen Sie Weiter.
17. (Optional) Geben Sie ein oder mehrere Tags für die Regel ein. Weitere Informationen finden Sie unter EventBridge Amazon-Tags im EventBridge Amazon-Benutzerhandbuch.
18. Wählen Sie Weiter.
19. Überprüfen Sie die Details der Regel und wählen Sie dann Create rule (Regel erstellen) aus.

    Wenn Sie eine benutzerdefinierte Aktion mit Ergebnissen oder Insight-Ergebnissen in Ihrem Konto durchführen, werden Ereignisse in generiert EventBridge.

Auswahl einer benutzerdefinierten Aktion für Ergebnisse und Insight-Ergebnisse

Nachdem Sie Ihre benutzerdefinierten Aktionen und EventBridge Regeln für Security Hub erstellt haben, können Sie Ergebnisse und Insight-Ergebnisse EventBridge zur weiteren Verwaltung und Verarbeitung an diese senden.

Ereignisse werden EventBridge nur an das Konto gesendet, in dem sie angesehen werden. Wenn Sie sich ein Ergebnis mit einem Administratorkonto ansehen, wird das Ereignis EventBridge an das Administratorkonto gesendet.

Damit AWS API-Aufrufe wirksam sind, müssen bei den Implementierungen des Zielcodes Rollen in Mitgliedskonten umgewandelt werden. Das bedeutet auch, dass die Rolle, in die Sie wechseln, für jedes Mitglied bereitgestellt werden muss, bei dem Maßnahmen erforderlich sind.

Um Ergebnisse zu senden an EventBridge

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/.
2. Eine Liste mit Ergebnissen anzeigen:
   - Unter Ergebnisse können Sie die Ergebnisse aller aktivierten Produktintegrationen und Kontrollen einsehen.
   - Unter Sicherheitsstandards können Sie zu einer Liste mit Ergebnissen navigieren, die anhand einer ausgewählten Kontrolle generiert wurden. Siehe the section called “Details für ein Steuerelement anzeigen”.
   - Unter Integrationen können Sie zu einer Liste mit Ergebnissen navigieren, die von einer aktivierten Integration generiert wurden. Siehe the section called “Anzeigen der Ergebnisse einer Integration”.
   - In Insights können Sie zu einer Ergebnisliste für ein Insight-Ergebnis navigieren. Siehe the section called “Anzeigen von Insight-Ergebnissen und -Resultaten”.
3. Wählen Sie die Ergebnisse aus, an die Sie senden möchten EventBridge. Sie können bis zu 20 Ergebnisse gleichzeitig auswählen.
4. Wählen Sie unter Aktionen die benutzerdefinierte Aktion aus, die der anzuwendenden EventBridge Regel entspricht.

   Security Hub sendet für jeden Befund ein separates Ereignis Security Hub Findings — Custom Action.

Um Insight-Ergebnisse zu senden an EventBridge

1. Öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Insights aus.
3. Wählen Sie auf der Insights-Seite den Insight aus, der die Ergebnisse enthält, an die Sie senden möchten EventBridge.
4. Wählen Sie die Insight-Ergebnisse aus, an die Sie senden möchten EventBridge. Sie können bis zu 20 Ergebnisse gleichzeitig auswählen.

5. Wählen Sie unter Aktionen die benutzerdefinierte Aktion aus, die der anzuwendenden EventBridge Regel entspricht.

Produktintegrationen in AWS Security Hub

AWSSecurity Hub kann Sicherheitssuchdaten von verschiedenen AWS Diensten und von unterstützten AWS Partner Network (APN) -Sicherheitslösungen zusammenfassen. Diese Aggregation bietet einen umfassenden Überblick über Sicherheit und Compliance in Ihrer AWS gesamten Umgebung.

Sie können auch Ergebnisse senden, die aus Ihren eigenen benutzerdefinierten Sicherheitsprodukten generiert werden.

> **Important**
>
> Von den unterstützten Produktintegrationen AWS und Partner-Produktintegrationen empfängt und konsolidiert Security Hub nur Ergebnisse, die generiert wurden, nachdem Sie Security Hub in Ihrem aktiviert haben. AWS-Konten
> Der Service empfängt und konsolidiert nicht rückwirkend Sicherheitserkenntnisse, die vor der Aktivierung von Security Hub generiert wurden.

Einzelheiten dazu, wie Security Hub für aufgenommene Ergebnisse Gebühren berechnet, finden Sie unter Security Hub Hub-Preise.

Themen

Verwalten von Produktintegrationen

Die Seite Integrationen im AWS Management Console bietet Zugriff auf alle verfügbaren Integrationen AWS und Produktintegrationen von Drittanbietern. Die AWS Security Hub Hub-API bietet auch Funktionen, mit denen Sie Integrationen verwalten können.

> **Note**
>
> Einige Integrationen sind in allen Regionen nicht verfügbar. Wenn eine Integration in der aktuellen Region nicht unterstützt wird, ist sie nicht auf der Seite Integrationen aufgeführt. Weitere Informationen finden Sie auch unter the section called “Integrationen, die in China (Peking) und China (Ningxia) unterstützt werden” und the section called “Integrationen, die in AWS GovCloud (US-Ost) und (US-West) unterstützt werden AWS GovCloud ”.

Die Liste der Integrationen anzeigen und filtern (Konsole)

Auf der Seite Integrations (Integrationen) können Sie die Liste der Integrationen anzeigen und filtern.

So zeigen Sie die Liste der Integrationen an:

1. Öffnen Sie die AWS Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Security Hub-Navigationsbereich Integrationen aus.

Auf der Seite Integrations (Integrationen) werden zuerst die Integrationen mit anderen AWS -Services aufgeführt, gefolgt von den Integrationen mit Drittanbieterprodukten.

Für jede Integration enthält die Seite Integrations (Integrationen) die folgenden Informationen.

- Der Name des Unternehmens
- Der Name des Produkts.
- Eine Beschreibung der Integration.
- Die Kategorien, für die die Integration gilt
- So aktivieren Sie die Integration:
- Der aktuelle Status der Integration

Sie können die Liste filtern, indem Sie Text aus den folgenden Feldern eingeben.

- Unternehmensname
- Produktname
- Beschreibung der Integration

- Kategorien

Informationen zu Produktintegrationen anzeigen (Security Hub Hub-API, AWS CLI)

Um Informationen zu Produktintegrationen anzuzeigen, können Sie einen API-Aufruf oder den verwenden. AWS Command Line Interface Sie können Informationen zu allen Produktintegrationen oder Informationen zu den von Ihnen aktivierten Produktintegrationen anzeigen.

Um Informationen zu allen verfügbaren Produktintegrationen anzuzeigen (Security Hub Hub-API, AWS CLI)

- Security Hub API — Verwenden Sie den `DescribeProducts`Vorgang. Um eine bestimmte Produktintegration zu identifizieren, die zurückgegeben werden soll, verwenden Sie den `ProductArn` Parameter, um den Integrations-ARN bereitzustellen.
- AWS CLI— Führen Sie den Befehl in der `describe-products`Befehlszeile aus. Um eine bestimmte Produktintegration zu identifizieren, die zurückgegeben werden soll, geben Sie den Integrations-ARN an.

```
aws securityhub describe-products --product-arn "<integrationARN>"
```

Beispiel

```
aws securityhub describe-products --product-arn "arn:aws:securityhub:us-
east-1::product/3coresec/3coresec"
```

Um Informationen zu Produktintegrationen anzuzeigen, die Sie aktiviert haben (Security Hub API, AWS CLI)

- Security Hub API — Verwenden Sie den `ListEnabledProductsForImport`Vorgang.
- AWS CLI— Führen Sie den Befehl in der `list-enabled-products-for-import`Befehlszeile aus.

```
aws securityhub list-enabled-products-for-import
```

Aktivieren einer Integration

Auf der Seite Integrations (Integrationen) bietet jede Integration die erforderlichen Schritte, um die Integration zu ermöglichen.

Bei den meisten Integrationen mit anderen AWS Diensten besteht der einzige erforderliche Schritt darin, den anderen Dienst zu aktivieren. Die Integrationsinformationen enthalten einen Link zur Service-Homepage. Wenn Sie den anderen Dienst aktivieren, wird automatisch eine Berechtigung auf Ressourcenebene erstellt und angewendet, die es Security Hub ermöglicht, Ergebnisse aus dem Dienst zu empfangen.

Bei Produktintegrationen von Drittanbietern müssen Sie die Integration möglicherweise bei der AWS Marketplace erwerben und anschließend konfigurieren. Die Integrationsinformationen enthalten Links, um diese Aufgaben auszuführen.

Wenn mehrere Versionen eines Produkts verfügbar sind AWS Marketplace, wählen Sie die Version aus, die Sie abonnieren möchten, und klicken Sie dann auf Weiter zum Abonnieren. Einige Produkte bieten beispielsweise eine Standardversion und eine AWS GovCloud (US) Version an.

Wenn Sie eine Produktintegration aktivieren, wird dem Produktabonnement automatisch eine Ressourcenrichtlinie angefügt. Diese Ressourcenrichtlinie definiert die Berechtigungen, die Security Hub benötigt, um Ergebnisse aus diesem Produkt zu erhalten.

Deaktivieren und Aktivieren des Flows von Ergebnissen aus einer Integration (Konsole)

Auf der Seite Integrationen geben die Statusinformationen für Integrationen, die Ergebnisse senden, an, ob Sie derzeit Ergebnisse akzeptieren.

Wenn Sie keine Ergebnisse mehr akzeptieren möchten, wählen Sie Stop accepting findings (Ergebnisse nicht akzeptieren) aus.

Um das Annehmen von Ergebnissen fortzusetzen, wählen Sie Accept findings (Ergebnisse akzeptieren) aus.

Den Fluss von Erkenntnissen aus einer Integration deaktivieren (Security Hub API, AWS CLI)

Um den Fluss der Ergebnisse einer Integration zu deaktivieren, können Sie einen API-Aufruf oder den AWS Command Line Interface verwenden.

Um den Fluss von Ergebnissen aus einer Integration zu deaktivieren (Security Hub API, AWS CLI)

- Security Hub API — Verwenden Sie den DisableImportFindingsForProductVorgang. Um die zu deaktivierende Integration zu identifizieren, benötigen Sie den ARN Ihres Abonnements. Verwenden Sie den Vorgang, um die Abonnement-ARNs für Ihre aktivierten Integrationen ListEnabledProductsForImportabzurufen.
- AWS CLI— Führen Sie den Befehl in der Befehlszeile aus. disable-import-findings-for-product

```
aws securityhub disable-import-findings-for-product --product-subscription-
arn <subscription ARN>
```

Beispiel

```
aws securityhub disable-import-findings-for-product --product-subscription-arn
 "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/
crowdstrike-falcon"
```

Den Fluss von Erkenntnissen aus einer Integration ermöglichen (Security Hub Hub-API, AWS CLI)

Um den Fluss von Erkenntnissen aus einer Integration zu ermöglichen, können Sie einen API-Aufruf oder den verwenden AWS Command Line Interface.

Um den Fluss von Erkenntnissen aus einer Integration zu ermöglichen (Security Hub Hub-API, AWS CLI)

- Security Hub API — Verwenden Sie den EnableImportFindingsForProductVorgang. Damit Security Hub Ergebnisse aus einer Integration empfangen kann, benötigen Sie das Produkt ARN. Verwenden Sie den Vorgang, um die ARNs für die verfügbaren Integrationen DescribeProductsabzurufen.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl enable-import-findings-for-product aus.

```
aws securityhub enable-import-findings-for-product --product-arn <integration ARN>
```

Beispiel

```
aws securityhub enable-import-findings-for product --product-arn
 "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

Anzeigen der Ergebnisse einer Integration

Für Integrationen, für die Sie Ergebnisse akzeptieren (Status ist „Ergebnisse werden akzeptiert“), wählen Sie Ergebnisse anzeigen aus, um eine Liste der Ergebnisse anzuzeigen.

Die Ergebnisliste zeigt die aktiven Ergebnisse für die ausgewählte Integration mit dem Workflow-Status `NEW` oder `NOTIFIED`.

Wenn Sie die regionsübergreifende Aggregation aktivieren, enthält die Liste in der Aggregationsregion Ergebnisse aus der Aggregationsregion und aus verknüpften Regionen, in denen die Integration aktiviert ist. Security Hub aktiviert Integrationen nicht automatisch, die auf der regionsübergreifenden Aggregationskonfiguration basieren.

In anderen Regionen enthält die Ergebnisliste für eine Integration nur Ergebnisse aus der aktuellen Region.

Informationen zur Konfiguration der regionsübergreifenden Aggregation finden Sie unter. Regionsübergreifende Aggregation

In der Ergebnisliste können Sie die folgenden Aktionen ausführen.

- Ändern der Filter und Gruppierung für die Liste
- Anzeigen der Details für einzelne Ergebnisse
- Aktualisieren des Workflow-Status der Ergebnisse
- Senden der Ergebnisse an benutzerdefinierte Aktionen

AWS-Service Integrationen mit AWS Security Hub

AWS Security Hub unterstützt Integrationen mit mehreren anderen AWS-Services.

> **Note**
>
> Einige Integrationen sind nur in ausgewählten Versionen verfügbar. AWS-Regionen

Wenn eine Integration in einer bestimmten Region nicht unterstützt wird, ist sie nicht auf der Seite Integrationen der Security Hub Hub-Konsole aufgeführt.
Weitere Informationen finden Sie unter Integrationen, die in China (Peking) und China (Ningxia) unterstützt werden und Integrationen, die in AWS GovCloud (US-Ost) und (US-West) unterstützt werden AWS GovCloud .

Sofern unten nicht anders angegeben, werden AWS-Service Integrationen, die Ergebnisse an Security Hub senden, automatisch aktiviert, nachdem Sie Security Hub aktiviert haben. Integrationen, die Security Hub Hub-Ergebnisse erhalten, erfordern möglicherweise zusätzliche Schritte zur Aktivierung. Lesen Sie die Informationen zu den einzelnen Integrationen, um mehr zu erfahren.

Überblick über die AWS Serviceintegrationen mit Security Hub

Hier finden Sie eine Übersicht über AWS Dienste, die Ergebnisse an Security Hub senden oder Ergebnisse von Security Hub empfangen.

Integrierter AWS Service	Richtung
AWS Config	Sendet Ergebnisse
AWS Firewall Manager	Sendet Ergebnisse
Amazon GuardDuty	Sendet Ergebnisse
AWS Health	Sendet Ergebnisse
AWS Identity and Access Management Access Analyzer	Sendet Ergebnisse
Amazon Inspector	Sendet Ergebnisse
AWS IoT Device Defender	Sendet Ergebnisse
Amazon Macie	Sendet Ergebnisse
AWS Systems Manager Patchmanager	Sendet Ergebnisse
AWS Audit Manager	Empfängt Ergebnisse

Integrierter AWS Service	Richtung
AWS Chatbot	Erhält Ergebnisse
Amazon Detective	Erhält Ergebnisse
Amazon Security Lake	Erhält Ergebnisse
AWS Systems Manager Explorer und OpsCenter	Empfängt und aktualisiert die Ergebnisse
AWS Trusted Advisor	Erhält Ergebnisse

AWS Dienste, die Ergebnisse an Security Hub senden

Die folgenden AWS Dienste lassen sich in Security Hub integrieren, indem sie Ergebnisse an Security Hub senden. Security Hub wandelt die Ergebnisse in das AWS Security Finding Format um.

AWS Config (Sendet Ergebnisse)

AWS Config ist ein Service, mit dem Sie die Konfigurationen Ihrer AWS Ressourcen bewerten, prüfen und auswerten können. AWS Config überwacht und zeichnet Ihre AWS Ressourcenkonfigurationen kontinuierlich auf und ermöglicht es Ihnen, die Auswertung der aufgezeichneten Konfigurationen anhand der gewünschten Konfigurationen zu automatisieren.

Wenn Sie die Integration mit verwenden AWS Config, können Sie die Ergebnisse AWS Config verwalteter und benutzerdefinierter Regelauswertungen als Ergebnisse in Security Hub anzeigen. Diese Erkenntnisse lassen sich zusammen mit anderen Ergebnissen von Security Hub aufrufen und bieten so einen umfassenden Überblick über Ihren Sicherheitsstatus.

AWS Config verwendet Amazon EventBridge , um AWS Config Regelauswertungen an Security Hub zu senden. Security Hub wandelt die Regelauswertungen in Ergebnisse um, die dem AWS Security Finding Format entsprechen. Security Hub bereichert die Ergebnisse dann nach bestem Wissen und Gewissen, indem es weitere Informationen über die betroffenen Ressourcen erhält, z. B. den Amazon-Ressourcennamen (ARN) und das Erstellungsdatum. Ressourcen-Tags in AWS Config Regelauswertungen sind nicht in den Ergebnissen von Security Hub enthalten.

Weitere Informationen zu dieser Integration finden Sie in den folgenden Abschnitten.

Wie AWS Config sendet Ergebnisse an Security Hub

Alle Ergebnisse in Security Hub verwenden das Standard-JSON-Format von ASFF. ASFF enthält Details zur Herkunft des Befundes, zur betroffenen Ressource und zum aktuellen Status des Ergebnisses. AWS Config sendet verwaltete und benutzerdefinierte Regelauswertungen an Security Hub über EventBridge. Security Hub wandelt die Regelbeurteilungen in Ergebnisse um, die sich an ASFF orientieren, und bereichert die Ergebnisse nach bestem Wissen und Gewissen.

Arten von Ergebnissen, die AWS Config an Security Hub gesendet werden

Sobald die Integration aktiviert ist, werden Bewertungen aller AWS Config verwalteten Regeln und benutzerdefinierten Regeln an Security Hub AWS Config gesendet. Nur Bewertungen von AWS Config Regeln, die mit Diensten verknüpft sind, wie sie beispielsweise zur Überprüfung von Sicherheitskontrollen verwendet werden, sind ausgeschlossen.

AWS Config Ergebnisse an Security Hub senden

Wenn die Integration aktiviert ist, weist Security Hub automatisch die Berechtigungen zu, die für den Empfang von Ergebnissen erforderlich sind AWS Config. Security Hub verwendet service-to-service Level-Berechtigungen, die Ihnen eine sichere Möglichkeit bieten, diese Integration zu aktivieren und Ergebnisse von AWS Config Amazon zu importieren EventBridge.

Latenz für das Senden von Erkenntnissen

Wenn ein neues Ergebnis AWS Config erstellt wird, können Sie das Ergebnis normalerweise innerhalb von fünf Minuten im Security Hub anzeigen.

Wiederholen, wenn der Security Hub nicht verfügbar ist

AWS Config sendet die Ergebnisse nach bestem Wissen und Gewissen an Security Hub. EventBridge Wenn ein Ereignis nicht erfolgreich an Security Hub übermittelt wurde, wird die EventBridge Zustellung bis zu 24 Stunden oder 185 Mal wiederholt, je nachdem, was zuerst eintritt.

Aktualisierung vorhandener AWS Config Ergebnisse in Security Hub

Nachdem ein Ergebnis an Security Hub AWS Config gesendet wurde, kann es Updates zu demselben Ergebnis an Security Hub senden, um zusätzliche Beobachtungen der Findungsaktivität widerzuspiegeln. Updates werden nur für `ComplianceChangeNotification` Ereignisse gesendet. Wenn keine Änderung der Konformität erfolgt, werden keine Updates an Security Hub gesendet. Security Hub löscht Ergebnisse 90 Tage nach dem letzten Update oder 90 Tage nach der Erstellung, wenn kein Update erfolgt.

Security Hub archiviert keine Ergebnisse, die gesendet wurden, AWS Config selbst wenn Sie die zugehörige Ressource löschen.

Regionen, in denen AWS Config Ergebnisse vorliegen

AWS Config Die Ergebnisse erfolgen auf regionaler Basis. AWS Config sendet Ergebnisse an Security Hub in derselben Region oder Regionen, in denen die Ergebnisse auftreten.

AWS Config Ergebnisse im Security Hub anzeigen

Um Ihre AWS Config Ergebnisse anzuzeigen, wählen Sie Findings im Security Hub-Navigationsbereich aus. Um die Ergebnisse so zu filtern, dass nur AWS Config Ergebnisse angezeigt werden, wählen Sie in der Dropdownliste der Suchleiste die Option Produktname aus. Geben Sie Config ein und wählen Sie Apply aus.

Interpretieren AWS Config von gefundenen Namen in Security Hub

Security Hub wandelt AWS Config Regelauswertungen in Ergebnisse um, die dem AWS Format für Sicherheitssuche (ASFF) folgen. AWS Config Regelauswertungen verwenden ein anderes Ereignismuster als ASFF. In der folgenden Tabelle werden die Felder für die AWS Config Regelauswertung ihrem ASFF-Gegenstück zugeordnet, so wie sie in Security Hub angezeigt werden.

Findetyp für die Auswertung der Konfigurationsregel	ASFF-Ergebnistyp	Hartcodierter Wert
Detail. awsAccountId	AwsAccountId	
Detail. newEvaluationResult. resultRecordedTime	CreatedAt	
Detail. newEvaluationResult. resultRecordedTime	UpdatedAt	
	ProductArn	<region>„arn ::securityhub:: <partition>:product/aws/config“
	ProductName	„Config“
	CompanyName	"AWS"
	Region	„eu-central-1"

Findetyp für die Auswertung der Konfigurationsregel	ASFF-Ergebnistyp	Hartcodierter Wert
configRuleArn	GeneratorId, ProductFields	
Detail. ConfigRuleARN/Finden/Hash	Id	
Detail. configRuleName	Titel, ProductFields	
Detail. configRuleName	Beschreibung	„Dieses Ergebnis wurde für eine Änderung der Ressourcenkonformität für die Konfigurationsregel erstellt:`${detail.ConfigRuleName}` “
Konfigurationselement „ARN“ oder von Security Hub berechneter ARN	Ressourcen [i] .id	
detail.Ressourcentyp	Ressourcen [i] .Type	"AwsS3Bucket"
	Ressourcen [i] .Partition	"aws"
	Ressourcen [i] .Region	„eu-central-1"
Konfigurationselement „Konfiguration“	Ressourcen [i] .Details	
	SchemaVersion	„2018-10-08"
	Schweregrad. Bezeichnung	Weitere Informationen finden Sie weiter unten unter „Interpretation des Schweregrads“
	Typen	["Software- und Konfigurationsprüfungen"]

Findetyp für die Auswertung der Konfigurationsregel	ASFF-Ergebnistyp	Hartcodierter Wert
Detail. newEvaluationResult. Art der Konformität	Konformität. Status	„FEHLGESCHLAGEN“, „NOT_AVAILABLE“, „BESTANDEN“ oder „WARNUNG“
	Arbeitsablauf.Status	„RESOLVED“, wenn ein AWS Config Ergebnis mit dem Wert Compliance.Status auf „PASSED“ generiert wird oder wenn sich der Wert Complianc e.Status von „FAILED“ auf „PASSED“ ändert. Andernfalls lautet Workflow.Status „NEW“. Sie können diesen Wert mit der BatchUpdateFindingsAPI-Operation ändern.

Interpretation der Bezeichnung des Schweregrads

Für alle Ergebnisse aus AWS Config Regelauswertungen ist in der ASFF standardmäßig der Schweregrad MITTEL angegeben. Sie können den Schweregrad eines Ergebnisses mit dem `BatchUpdateFindings`API-Vorgang aktualisieren.

Typischer Befund von AWS Config

Security Hub wandelt AWS Config Regelauswertungen in Ergebnisse um, die dem ASFF folgen. Im Folgenden finden Sie ein Beispiel für ein typisches Ergebnis aus AWS Config der ASFF.

> **Note**
>
> Wenn die Beschreibung mehr als 1024 Zeichen umfasst, wird sie auf 1024 Zeichen gekürzt und am Ende steht „(gekürzt)“.

```
{
```

```
 "SchemaVersion": "2018-10-08",
 "Id": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/45g070df80cb50b68fa6a43594kc6fda1e517932",
 "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/config",
 "ProductName": "Config",
 "CompanyName": "AWS",
 "Region": "eu-central-1",
 "GeneratorId": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-
mburzq",
 "AwsAccountId": "123456789012",
 "Types": [
  "Software and Configuration Checks"
 ],
 "CreatedAt": "2022-04-15T05:00:37.181Z",
 "UpdatedAt": "2022-04-19T21:20:15.056Z",
 "Severity": {
  "Label": "MEDIUM",
  "Normalized": 40
 },
 "Title": "s3-bucket-level-public-access-prohibited-config-integration-demo",
 "Description": "This finding is created for a resource compliance change for config
 rule: s3-bucket-level-public-access-prohibited-config-integration-demo",
 "ProductFields": {
  "aws/securityhub/ProductName": "Config",
  "aws/securityhub/CompanyName": "AWS",
  "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
config/arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/46f070df80cd50b68fa6a43594dc5fda1e517902",
  "aws/config/ConfigRuleArn": "arn:aws:config:eu-central-1:123456789012:config-rule/
config-rule-mburzq",
  "aws/config/ConfigRuleName": "s3-bucket-level-public-access-prohibited-config-
integration-demo",
  "aws/config/ConfigComplianceType": "NON_COMPLIANT"
 },
 "Resources": [{
  "Type": "AwsS3Bucket",
  "Id": "arn:aws:s3:::config-integration-demo-bucket",
  "Partition": "aws",
  "Region": "eu-central-1",
  "Details": {
   "AwsS3Bucket": {
    "OwnerId": "4edbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
    "CreatedAt": "2022-04-15T04:32:53.000Z"
   }
```

```
  }
 }],
 "Compliance": {
  "Status": "FAILED"
 },
 "WorkflowState": "NEW",
 "Workflow": {
  "Status": "NEW"
 },
 "RecordState": "ACTIVE",
 "FindingProviderFields": {
  "Severity": {
   "Label": "MEDIUM"
  },
  "Types": [
   "Software and Configuration Checks"
  ]
 }
}
```

Aktivieren und Konfigurieren der Integration

Nachdem Sie Security Hub aktiviert haben, wird diese Integration automatisch aktiviert. AWS Config beginnt sofort, Ergebnisse an Security Hub zu senden.

Einstellung der Veröffentlichung von Erkenntnissen in Security Hub

Um das Senden von Ergebnissen an Security Hub zu beenden, können Sie die Security Hub Hub-Konsole, die Security Hub Hub-API oder die verwenden AWS CLI.

Weitere Informationen unter Deaktivieren und Aktivieren des Flows von Ergebnissen aus einer Integration (Konsole) oder Den Fluss von Erkenntnissen aus einer Integration deaktivieren (Security Hub API, AWS CLI).

AWS Firewall Manager (Sendet Ergebnisse)

Firewall Manager sendet Ergebnisse an Security Hub, wenn eine Web Application Firewall (WAF) -Richtlinie für Ressourcen oder eine Web Access Control List (Web ACL) -Regel nicht den Vorschriften entspricht. Firewall Manager sendet auch Erkenntnisse, wenn AWS Shield Advanced Ressourcen nicht geschützt sind oder wenn ein Angriff erkannt wird.

Nachdem Sie Security Hub aktiviert haben, wird diese Integration automatisch aktiviert. Firewall Manager beginnt sofort, Ergebnisse an Security Hub zu senden.

Weitere Informationen zur Integration finden Sie auf der Seite Integrationen in der Security Hub Hub-Konsole.

Weitere Informationen zu Firewall Manager finden Sie im AWS WAF Entwicklerhandbuch.

Amazon GuardDuty (Sendet Ergebnisse)

GuardDuty sendet alle Ergebnisse, die es generiert, an Security Hub.

Neue Ergebnisse von GuardDuty werden innerhalb von fünf Minuten an Security Hub gesendet. Aktualisierungen der Ergebnisse werden auf der Grundlage der Einstellung Aktualisierte Ergebnisse für Amazon EventBridge in den GuardDuty Einstellungen gesendet.

Wenn Sie GuardDuty Stichprobenergebnisse mithilfe der GuardDuty Einstellungsseite generieren, empfängt Security Hub die Probenergebnisse und lässt das Präfix `[Sample]` im Befundtyp weg. Beispielsweise GuardDuty `[SAMPLE] Recon:IAMUser/ResourcePermissions` wird der Suchtyp der Stichprobe in wie `Recon:IAMUser/ResourcePermissions` in Security Hub angezeigt.

Nachdem Sie Security Hub aktiviert haben, wird diese Integration automatisch aktiviert. GuardDuty beginnt sofort, Ergebnisse an Security Hub zu senden.

Weitere Informationen zur GuardDuty Integration finden Sie unter Integration mit AWS Security Hub im GuardDuty Amazon-Benutzerhandbuch.

AWS Health (Sendet Ergebnisse)

AWS Health bietet fortlaufenden Einblick in die Leistung Ihrer Ressourcen und die Verfügbarkeit Ihrer AWS Dienste und Konten. Anhand von AWS Health Ereignissen können Sie herausfinden, wie sich Änderungen an Diensten und Ressourcen auf Ihre Anwendungen auswirken können, die auf ausgeführt AWS werden.

Die Integration mit verwendet AWS Health nicht`BatchImportFindings`. AWS Health Verwendet stattdessen service-to-service Ereignisnachrichten, um Ergebnisse an Security Hub zu senden.

Weitere Informationen zur Integration finden Sie in den folgenden Abschnitten.

Wie AWS Health sendet Ergebnisse an Security Hub

Im Security Hub werden Sicherheitsprobleme als Erkenntnisse verfolgt. Einige Ergebnisse stammen aus Problemen, die von anderen AWS Diensten oder von Drittanbietern entdeckt wurden.

Security Hub verwendet ebenfalls verschiedene Regeln, um Sicherheitsprobleme zu erkennen und Ergebnisse zu generieren.

Security Hub bietet Tools zur Verwaltung von Erkenntnissen aus all diesen Quellen. Sie können Listen mit Erkenntnissen anzeigen und filtern und Details zu einer Erkenntnis anzeigen. Siehe Verwaltung und Überprüfung der Funddetails und des Verlaufs. Sie können auch den Status einer Untersuchung zu einer Erkenntnis nachverfolgen. Siehe Ergreifen von Maßnahmen aufgrund der Ergebnisse in AWS Security Hub.

Alle Ergebnisse in Security Hub verwenden ein Standard-JSON-Format namensAWS Format für Sicherheitssuche (ASFF). ASFF enthält Einzelheiten zur Ursache des Problems, zu den betroffenen Ressourcen und zum aktuellen Stand der Ergebnisse.

AWS Health ist einer der AWS Dienste, der Ergebnisse an Security Hub sendet.

Arten von Ergebnissen, die AWS Health an Security Hub gesendet werden

Sobald die Integration aktiviert ist, werden alle von ihr generierten sicherheitsrelevanten Ergebnisse an Security Hub AWS Health gesendet. Die Ergebnisse werden mit dem an Security Hub gesendetAWS Format für Sicherheitssuche (ASFF). Sicherheitsbezogene Ergebnisse sind wie folgt definiert:

- Jeder Befund im Zusammenhang mit einem Sicherheitsdienst AWS
- Jeder Befund mit den Wörtern`security`,`abuse`, oder `certificate` im AWS Health TypeCode
- Irgendein Befund, wo sich der AWS Health Dienst befindet `risk` oder `abuse`

AWS Health Ergebnisse an Security Hub senden

Wenn Sie sich dafür entscheiden, Ergebnisse von zu akzeptieren AWS Health, weist Security Hub automatisch die Berechtigungen zu, die für den Empfang der Ergebnisse von erforderlich sind AWS Health. Security Hub verwendet service-to-service Level-Berechtigungen, die Ihnen eine sichere und einfache Möglichkeit bieten, diese Integration zu aktivieren und Ergebnisse in Ihrem Namen AWS Health EventBridge über Amazon zu importieren. Wenn Sie „Ergebnisse akzeptieren“ wählen, erteilt Security Hub die Erlaubnis, Ergebnisse von zu verwenden AWS Health.

Latenz für das Senden von Erkenntnissen

Wenn ein neues Ergebnis AWS Health erstellt wird, wird es normalerweise innerhalb von fünf Minuten an Security Hub gesendet.

Wiederholen, wenn der Security Hub nicht verfügbar ist

AWS Health sendet die Ergebnisse nach bestem Wissen und Gewissen an Security Hub. EventBridge Wenn ein Ereignis nicht erfolgreich an Security Hub übermittelt wurde, wird EventBridge erneut versucht, das Ereignis für 24 Stunden zu senden.

Aktualisieren von vorhandenen Erkenntnissen in Security Hub

Nachdem ein Ergebnis an Security Hub AWS Health gesendet wurde, kann es Updates zu demselben Ergebnis senden, um zusätzliche Beobachtungen der Findungsaktivität an Security Hub widerzuspiegeln.

Regionen, in denen Ergebnisse vorliegen

AWS Health Sendet bei globalen Ereignissen Ergebnisse an Security Hub in us-east-1 (AWS Partition), cn-northwest-1 (Partition China) und -1 (Partition). gov-us-west GovCloud AWS Health sendet regionsspezifische Ereignisse an Security Hub in derselben Region oder Regionen, in denen die Ereignisse auftreten.

AWS Health Ergebnisse im Security Hub anzeigen

Um Ihre AWS Health Ergebnisse in Security Hub anzuzeigen, wählen Sie im Navigationsbereich Findings aus. Um die Ergebnisse so zu filtern, dass nur AWS Health Ergebnisse angezeigt werden, wählen Sie Health aus dem Feld Produktname aus.

Interpretieren AWS Health von gefundenen Namen in Security Hub

AWS Health sendet die Ergebnisse mit dem an Security HubAWS Format für Sicherheitssuche (ASFF). AWS Health Die Suche verwendet ein anderes Ereignismuster als das Security Hub ASFF-Format. In der folgenden Tabelle sind alle Ergebnisfelder AWS Health mit ihren ASFF-Gegenstücken aufgeführt, so wie sie in Security Hub erscheinen.

Art Health Gesundheitsbefundung	ASFF-Ergebnistyp	Hartcodierter Wert
Konto	AwsAccountId	
Detail.StartTime	CreatedAt	
Detail.EventDescription.Letzte Beschreibung	Beschreibung	

Art Health Gesundheitsbefundung	ASFF-Ergebnistyp	Hartcodierter Wert
Detail. eventTypeCode	GeneratorId	
detail.eventArn (einschließlich Konto) + Hash von detail.StartTime	Id	
<region>„arn:aws:securityhub:: :product/aws/health“	ProductArn	
Konto oder resourceId	Ressourcen [i] .id	
	Ressourcen [i] .Type	„Andere“
	SchemaVersion	„2018-10-08"
	Schweregrad. Bezeichnung	Weitere Informationen finden Sie weiter unten unter „Interpretation des Schweregrads“
Detail „AWS Health -“. eventTypeCode	Title	
-	Typen	["Software- und Konfigurationsprüfungen"]
event.time	UpdatedAt	
URL des Ereignisses auf der Health Console	SourceUrl	

Interpretation des Schweregrads

Der Schweregrad im ASFF-Ergebnis wird anhand der folgenden Logik bestimmt:

- Schweregrad KRITISCH wenn:

- Das `service` Feld im AWS Health Ergebnis hat den Wert `Risk`
- Das `typeCode` Feld im AWS Health Befund hat den Wert `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`
- Das `typeCode` Feld im AWS Health Befund hat den Wert `AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK`
- Das `typeCode` Feld im AWS Health Befund hat den Wert `AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES`

Schweregrad HOCH, wenn:

- Das `service` Feld im AWS Health Ergebnis hat den Wert `Abuse`
- Das `typeCode` Feld im AWS Health Befund enthält den Wert `SECURITY_NOTIFICATION`
- Das `typeCode` Feld im AWS Health Befund enthält den Wert `ABUSE_DETECTION`

Schweregrad MITTEL, wenn:

- Das `service` Feld im Ergebnis ist eines der folgenden:`ACM`,,,,,,,`ARTIFACT`,`AUDITMANAGER`,`BACKUP`,,`CLOUDENDURE`,`CLOUDHSM`,`CLOUDTRAIL`,,`CLOU` oder `WAF`
- Das TypeCode-Feld im AWS Health Ergebnis enthält den Wert `CERTIFICATE`
- Das TypeCode-Feld im AWS Health Befund enthält den Wert `END_OF_SUPPORT`

Typischer Befund von AWS Health

AWS Health sendet Ergebnisse mit dem an Security HubAWS Format für Sicherheitssuche (ASFF). Im Folgenden finden Sie ein Beispiel für ein typisches Ergebnis von AWS Health.

> **Note**
>
> Wenn die Beschreibung mehr als 1024 Zeichen umfasst, wird sie auf 1024 Zeichen gekürzt und am Ende steht (gekürzt).

```
{
            "SchemaVersion": "2018-10-08",
            "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
```

```
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
            "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
            "AwsAccountId": "123456789012",
            "Types": [
                "Software and Configuration Checks"
            ],
            "CreatedAt": "2022-01-07T16:34:04.000Z",
            "UpdatedAt": "2022-01-07T19:17:43.000Z",
            "Severity": {
                "Label": "MEDIUM",
                "Normalized": 40
            },
            "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
            "Description": "Congratulations! Amazon SES has successfully detected the
 MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\\n\\nYou can now use this MAIL
 FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity
 that is configured to use it. For information about how to configure a verified
 identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/
DeveloperGuide/mail-from-set.html .\\n\\nPlease note that this email only applies to
 AWS Region US East (N. Virginia).",
            "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
            "ProductFields": {
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
                "aws/securityhub/ProductName": "Health",
                "aws/securityhub/CompanyName": "AWS"
            },
            "Resources": [
                {
                    "Type": "Other",
                    "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
                }
            ],
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NEW"
```

```
            },
            "RecordState": "ACTIVE",
            "FindingProviderFields": {
                "Severity": {
                    "Label": "MEDIUM"
                },
                "Types": [
                    "Software and Configuration Checks"
                ]
            }
        }
    ]
}
```

Aktivieren und Konfigurieren der Integration

Nachdem Sie Security Hub aktiviert haben, wird diese Integration automatisch aktiviert. AWS Health beginnt sofort, Ergebnisse an Security Hub zu senden.

Einstellung der Veröffentlichung von Erkenntnissen in Security Hub

Um das Senden von Ergebnissen an Security Hub zu beenden, können Sie die Security Hub Hub-Konsole, die Security Hub Hub-API oder verwenden AWS CLI.

Weitere Informationen unter Deaktivieren und Aktivieren des Flows von Ergebnissen aus einer Integration (Konsole) oder Den Fluss von Erkenntnissen aus einer Integration deaktivieren (Security Hub API, AWS CLI).

AWS Identity and Access Management Access Analyzer (Sendet Ergebnisse)

Mit IAM Access Analyzer werden alle Ergebnisse an Security Hub gesendet.

IAM Access Analyzer analysiert anhand von logischer Argumentation ressourcenbasierte Richtlinien, die auf unterstützte Ressourcen in Ihrem Konto angewendet werden. IAM Access Analyzer generiert ein Ergebnis, wenn er eine Richtlinienaussage entdeckt, die einem externen Principal den Zugriff auf eine Ressource in Ihrem Konto ermöglicht.

In IAM Access Analyzer kann nur das Administratorkonto Ergebnisse für Analyzer sehen, die für eine Organisation gelten. Bei Organisationsanalyseprogrammen gibt das `AwsAccountId` ASFF-Feld die Administratorkonto-ID an. Das `ResourceOwnerAccount` Feld `ProductFields` darunter gibt das Konto an, in dem das Ergebnis entdeckt wurde. Wenn Sie Analyzer für jedes Konto

einzeln aktivieren, generiert Security Hub mehrere Ergebnisse, eines, das die Administratorkonto-ID identifiziert, und eines, das die Ressourcenkonto-ID identifiziert.

Weitere Informationen finden Sie unter Integration mit AWS Security Hub im IAM-Benutzerhandbuch.

Amazon Inspector (Sendet Ergebnisse)

Amazon Inspector ist ein Schwachstellen-Management-Service, der Ihre AWS Workloads kontinuierlich auf Sicherheitslücken scannt. Amazon Inspector erkennt und scannt automatisch Amazon EC2 EC2-Instances und Container-Images, die sich in der Amazon Elastic Container Registry befinden. Der Scan sucht nach Softwareschwachstellen und unbeabsichtigten Netzwerkbedrohungen.

Nachdem Sie Security Hub aktiviert haben, wird diese Integration automatisch aktiviert. Amazon Inspector beginnt sofort, alle Ergebnisse, die es generiert, an Security Hub zu senden.

Weitere Informationen zur Integration finden Sie unter Integration mit AWS Security Hub im Amazon Inspector Inspector-Benutzerhandbuch.

Security Hub kann auch Ergebnisse von Amazon Inspector Classic erhalten. Amazon Inspector Classic sendet Ergebnisse an Security Hub, die im Rahmen von Bewertungsläufen für alle unterstützten Regelpakete generiert wurden.

Weitere Informationen zur Integration finden Sie unter Integration mit AWS Security Hub im Amazon Inspector Classic-Benutzerhandbuch.

Die Ergebnisse für Amazon Inspector und Amazon Inspector Classic verwenden denselben Produkt-ARN. Die Ergebnisse von Amazon Inspector haben den folgenden Eintrag in`ProductFields`:

```
"aws/inspector/ProductVersion": "2",
```

AWS IoT Device Defender (Sendet Ergebnisse)

AWS IoT Device Defender ist ein Sicherheitsdienst, der die Konfiguration Ihrer IoT-Geräte überprüft, angeschlossene Geräte überwacht, um ungewöhnliches Verhalten zu erkennen, und zur Minderung von Sicherheitsrisiken beiträgt.

Nachdem Sie beide AWS IoT Device Defender und Security Hub aktiviert haben, rufen Sie die Integrationsseite der Security Hub Hub-Konsole auf und wählen Sie Ergebnisse akzeptieren für Audit, Detect oder beides aus. AWS IoT Device Defender Audit and Detect beginnt, alle Ergebnisse an Security Hub zu senden.

AWS IoT Device Defender Audit sendet Prüfzusammenfassungen an Security Hub, die allgemeine Informationen für einen bestimmten Prüfungstyp und eine bestimmte Prüfungsaufgabe enthalten. AWS IoT Device Defender Detect sendet festgestellte Verstöße für maschinelles Lernen (ML), statistisches und statisches Verhalten an Security Hub. Audit sendet auch gefundene Updates an Security Hub.

Weitere Informationen zu dieser Integration finden Sie unter Integration mit AWS Security Hub im AWS IoT Entwicklerhandbuch.

Amazon Macie (Sendet Ergebnisse)

Ein Ergebnis von Macie kann darauf hinweisen, dass ein potenzieller Verstoß gegen die Richtlinien vorliegt oder dass sensible Daten, wie z. B. personenbezogene Daten (PII), in Daten enthalten sind, die Ihre Organisation in Amazon S3 speichert.

Nachdem Sie Security Hub aktiviert haben, beginnt Macie automatisch, Richtlinienergebnisse an Security Hub zu senden. Sie können die Integration so konfigurieren, dass auch Ergebnisse vertraulicher Daten an Security Hub gesendet werden.

In Security Hub wird der Suchtyp für eine Richtlinie oder einen Fund vertraulicher Daten auf einen Wert geändert, der mit ASFF kompatibel ist. Beispielsweise wird der `Policy:IAMUser/S3BucketPublic` Findungstyp in Macie wie `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic` in Security Hub angezeigt.

Macie sendet auch generierte Probenergebnisse an Security Hub. Bei Stichprobenergebnissen lautet der Name der betroffenen Ressource `macie-sample-finding-bucket` und der Wert für das `Sample` Feld lautet`true`.

Weitere Informationen finden Sie unter Amazon Macie Macie-Integration mit AWS Security Hub im Amazon Macie Macie-Benutzerhandbuch.

AWS Systems Manager Patch Manager (Sendet Ergebnisse)

AWS Systems Manager Patch Manager sendet Ergebnisse an Security Hub, wenn Instances in der Flotte eines Kunden nicht mehr dem Patch-Compliance-Standard entsprechen.

Patch Manager automatisiert den Prozess des Patchens verwalteter Instanzen mit sicherheitsrelevanten und anderen Arten von Updates.

Nachdem Sie Security Hub aktiviert haben, wird diese Integration automatisch aktiviert. Systems Manager Patch Manager beginnt sofort, Ergebnisse an Security Hub zu senden.

Weitere Informationen zur Verwendung von Patch Manager finden Sie unter AWS Systems Manager Patch Manager im AWS Systems Manager Benutzerhandbuch.

AWS Dienste, die Erkenntnisse von Security Hub erhalten

Die folgenden AWS Dienste sind in Security Hub integriert und beziehen Ergebnisse von Security Hub. Sofern angegeben, kann der integrierte Dienst die Ergebnisse auch aktualisieren. In diesem Fall wird das Auffinden von Updates, die Sie im integrierten Dienst vornehmen, auch in Security Hub widergespiegelt.

AWS Audit Manager (Erhält Ergebnisse)

AWS Audit Manager erhält Ergebnisse von Security Hub. Diese Ergebnisse helfen den Benutzern von Audit Manager, sich auf Audits vorzubereiten.

Weitere Informationen zu Audit Manager finden Sie im AWS Audit Manager Manager-Benutzerhandbuch. AWS Security Hub-Prüfungen, die von unterstützt werden, AWS Audit Manager listet die Kontrollen auf, für die Security Hub Ergebnisse an Audit Manager sendet.

AWS Chatbot (Empfängt Ergebnisse)

AWS Chatbot ist ein interaktiver Agent, der Ihnen hilft, Ihre AWS Ressourcen in Ihren Slack-Kanälen und Amazon Chime Chime-Chatrooms zu überwachen und mit ihnen zu interagieren.

AWS Chatbot erhält Ergebnisse von Security Hub.

Weitere Informationen zur AWS Chatbot Integration mit Security Hub finden Sie in der Security Hub Hub-Integrationsübersicht im AWS Chatbot Administratorhandbuch.

Amazon Detective (erhält Ergebnisse)

Detective sammelt automatisch Protokolldaten aus Ihren AWS Ressourcen und nutzt maschinelles Lernen, statistische Analysen und Graphentheorie, um Sie bei der Visualisierung und Durchführung schnellerer und effizienterer Sicherheitsuntersuchungen zu unterstützen.

Die Security Hub-Integration mit Detective ermöglicht es Ihnen, von GuardDuty Amazon-Ergebnissen in Security Hub zu Detective zu wechseln. Anschließend können Sie die Detective-Tools und Visualisierungen verwenden, um sie zu untersuchen. Die Integration erfordert keine zusätzliche Konfiguration in Security Hub oder Detective.

Für Ergebnisse, die von anderen stammen AWS-Services, enthält der Bereich mit den Befunddetails auf der Security Hub Hub-Konsole den Unterabschnitt In Detective untersuchen.

Dieser Unterabschnitt enthält einen Link zu Detective, über den Sie das Sicherheitsproblem, das durch den Befund gemeldet wurde, weiter untersuchen können. Sie können in Detective auch ein Verhaltensdiagramm erstellen, das auf den Ergebnissen von Security Hub basiert, um effektivere Untersuchungen durchzuführen. Weitere Informationen finden Sie in den AWS Sicherheitsergebnissen im Amazon Detective Administration Guide.

Wenn die regionsübergreifende Aggregation aktiviert ist und Sie von der Aggregationsregion aus wechseln, wird Detective in der Region geöffnet, aus der das Ergebnis stammt.

Wenn ein Link nicht funktioniert, finden Sie Hinweise zur Fehlerbehebung unter Troubleshooting the Pivot.

Amazon Security Lake (erhält Ergebnisse)

Security Lake ist ein vollständig verwalteter Sicherheits-Data-Lake-Service. Sie können Security Lake verwenden, um Sicherheitsdaten aus Cloud-, lokalen und benutzerdefinierten Quellen automatisch in einem Data Lake zu zentralisieren, der in Ihrem Konto gespeichert ist. Abonnenten können Daten aus Security Lake für Ermittlungs- und Analysezwecke nutzen.

Um diese Integration zu aktivieren, müssen Sie beide Dienste aktivieren und Security Hub als Quelle in der Security Lake-Konsole, der Security Lake-API oder hinzufügen AWS CLI. Sobald Sie diese Schritte abgeschlossen haben, beginnt Security Hub, alle Ergebnisse an Security Lake zu senden.

Security Lake normalisiert die Ergebnisse von Security Hub automatisch und konvertiert sie in ein standardisiertes Open-Source-Schema namens Open Cybersecurity Schema Framework (OCSF). In Security Lake können Sie einen oder mehrere Abonnenten hinzufügen, um die Ergebnisse von Security Hub zu nutzen.

Weitere Informationen zu dieser Integration, einschließlich Anweisungen zum Hinzufügen von Security Hub als Quelle und zum Erstellen von Abonnenten, finden Sie unter Integration mit AWS Security Hub im Amazon Security Lake-Benutzerhandbuch.

AWS Systems Manager Explorer und OpsCenter (Empfängt und aktualisiert Ergebnisse)

AWS Systems Manager Erkunden und OpsCenter empfangen Sie Ergebnisse von Security Hub und aktualisieren Sie diese Ergebnisse in Security Hub.

Explorer bietet Ihnen ein anpassbares Dashboard, das wichtige Einblicke und Analysen zum Betriebszustand und zur Leistung Ihrer AWS Umgebung bietet.

OpsCenter bietet Ihnen einen zentralen Ort, an dem Sie betriebliche Arbeitsaufgaben anzeigen, untersuchen und lösen können.

Weitere Informationen zu Explorer und OpsCenter finden Sie unter Operations Management im AWS Systems Manager Benutzerhandbuch.

AWS Trusted Advisor (Erhält Ergebnisse)

Trusted Advisor stützt sich auf bewährte Verfahren, die bei der Betreuung von Hunderttausenden von AWS Kunden gelernt wurden. Trusted Advisor untersucht Ihre AWS Umgebung und gibt dann Empfehlungen, wenn Möglichkeiten bestehen, Geld zu sparen, die Systemverfügbarkeit und -leistung zu verbessern oder Sicherheitslücken zu schließen.

Wenn Sie Trusted Advisor sowohl als auch Security Hub aktivieren, wird die Integration automatisch aktualisiert.

Security Hub sendet die Ergebnisse seiner AWS Foundational Security Best Practices-Prüfungen an Trusted Advisor.

Weitere Informationen zur Security Hub-Integration mit Trusted Advisor finden Sie unter AWS Security Hub-Steuerelemente anzeigen AWS Trusted Advisor im AWS Support-Benutzerhandbuch.

Verfügbare Integrationen von Produkten von Drittanbieterpartnern

AWS Security Hub lässt sich in mehrere Partnerprodukte von Drittanbietern integrieren. Eine Integration kann eine oder mehrere der folgenden Aktionen ausführen:

- Senden Sie die Ergebnisse, die es generiert, an Security Hub.
- Erhalten Sie Ergebnisse von Security Hub.
- Aktualisieren Sie die Ergebnisse im Security Hub.

Alle Integrationen, die Ergebnisse an Security Hub senden, haben einen Amazon-Ressourcennamen (ARN).

> **Note**
>
> Einige Integrationen sind nur in ausgewählten Versionen verfügbar. AWS-Regionen Auf der Seite Integrationen der Security Hub Hub-Konsole sind alle unterstützten Integrationen für die aktuelle Region aufgeführt.

Weitere Informationen finden Sie unter Integrationen, die in China (Peking) und China (Ningxia) unterstützt werden und Integrationen, die in AWS GovCloud (US-Ost) und (US-West) unterstützt werden AWS GovCloud .

Wenn Sie über eine Sicherheitslösung verfügen und daran interessiert sind, ein Security Hub-Partner zu werden, senden Sie eine E-Mail <an securityhub-partners@amazon.com>. Weitere Informationen finden Sie im AWS Security Hub Partner Integration Guide.

Überblick über Integrationen von Drittanbietern mit Security Hub

Hier finden Sie eine Übersicht über die Integrationen von Drittanbietern, die Ergebnisse an Security Hub senden oder Ergebnisse von Security Hub empfangen.

Integration	Richtung	ARN (falls zutreffend)
3CORESec – 3CORESec NTA	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/3coresec/3coresec`
Alert Logic – SIEMless Threat Management	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:733251395267:product/alertlogic/althreatmanagement`
Aqua Security – Aqua Cloud Native Security Platform	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/aquasecurity/aquasecurity`
Aqua Security – Kube-bench	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/aqua-security/kube-bench`
Armor – Armor Anywhere	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:67970361`

Integration	Richtung	ARN (falls zutreffend)
		5338:product/armor defense/armoranywh ere
AttackIQ – AttackIQ	Sendet Ergebnisse	arn:aws:securityhu b: *<REGION>*::product /attackiq/attackiq- platform
Barracuda Networks – Cloud Security Guardian	Sendet Ergebnisse	arn:aws:securityhu b: *<REGION>*:15178405 5945:product/barra cuda/cloudsecurity guardian
BigID – BigID Enterprise	Sendet Ergebnisse	arn:aws:securityhu b: *<REGION>*::product /bigid/bigid-enter prise
Blue Hexagon – Blue Hexagon forAWS	Sendet Ergebnisse	arn:aws:securityhu b: *<REGION>*::product /blue-hexagon/blue- hexagon-for-aws
Capitis Solutions – C2VS	Sendet Ergebnisse	arn:aws:securityhu b: *<REGION>*::product/ capitis/c2vs
Check Point – CloudGuard IaaS	Sendet Ergebnisse	arn:aws:securityhu b: *<REGION>*:75824556 3457:product/check point/cloudguard-i aas

Integration	Richtung	ARN (falls zutreffend)
Check Point – CloudGuard Posture Management	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:634729597623:product/checkpoint/dome9-arc`
Claroty – xDome	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/claroty/xdome`
Cloud Storage Security—Antivirus for Amazon S3	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`
Contrast Security	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/contrast-security/security-assess`
CrowdStrike – CrowdStrike Falcon	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`
CyberArk – Privileged Threat Analytics	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:749430749651:product/cyberark/cyberark-pta`
Data Theorem – Data Theorem	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/data-theorem/api-cloud-web-secure`

Integration	Richtung	ARN (falls zutreffend)
Drata	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/drata/drata-integration`
Forcepoint – Forcepoint CASB	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-casb`
Forcepoint – Forcepoint Cloud Security Gateway	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/forcepoint/forcepoint-cloud-security-gateway`
Forcepoint – Forcepoint DLP	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-dlp`
Forcepoint – Forcepoint NGFW	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-ngfw`
Fugue – Fugue	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/fugue/fugue`

Integration	Richtung	ARN (falls zutreffend)
Guardicore – Centra 4.0	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/guardicore/guardicore`
HackerOne – Vulnerability Intelligence	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/hackerone/vulnerability-intelligence`
JFrog – Xray	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/jfrog/jfrog-xray`
Juniper Networks – vSRX Next Generation Firewall	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/juniper-networks/vsrx-next-generation-firewall`
k9 Security – Access Analyzer	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/k9-security/access-analyzer`
Lacework – Lacework	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/lacework/lacework`
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

Integration	Richtung	ARN (falls zutreffend)
NETSCOUT – NETSCOUT Cyber Investigator	Sendet Ergebnisse	`arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator`
Palo Alto Networks – Prisma Cloud Compute	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:496947949261:product/twistlock/twistlock-enterprise`
Palo Alto Networks – Prisma Cloud Enterprise	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:188619942792:product/paloaltonetworks/redlock`
Plerion – Cloud Security Platform	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/plerion/cloud-security-platform`
Prowler – Prowler	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/prowler/prowler`
Qualys – Vulnerability Management	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:805950163170:product/qualys/qualys-vm`
Rapid7 – InsightVM	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:336818582268:product/rapid7/insightvm`

Integration	Richtung	ARN (falls zutreffend)
SecureCloudDB – SecureCloudDB	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/securecloudb/securecloudb`
SentinelOne – SentinelOne	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/sentinelone/endpoint-protection`
Snyk	Sendet Ergebnisse	`arn:aws:securityhub: <region>::product/snyk/snyk`
Sonrai Security – Sonrai Dig	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/sonrai-security/sonrai-dig`
Sophos – Server Protection	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:062897671886:product/sophos/sophos-server-protection`
StackRox – StackRox Kubernetes Security	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/stackrox/kubernetes-security`
Sumo Logic – Machine Data Analytics	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:956882708938:product/sumologicinc/sumologic-mda`

Integration	Richtung	ARN (falls zutreffend)
Symantec – Cloud Workload Protection	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:754237914691:product/symantec-corp/symantec-cwp`
Tenable – Tenable.io	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:422820575223:product/tenable/tenable-io`
Trend Micro – Cloud One	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/trend-micro/cloud-one`
Vectra – Cognito Detect	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>:978576646331:product/vectra-ai/cognito-detect`
Wiz	Sendet Ergebnisse	`arn:aws:securityhub: <REGION>::product/wiz-security/wiz-security`
Atlassian - Jira Service Management	Empfängt und aktualisiert Ergebnisse	Nicht zutreffend
Atlassian - Jira Service Management Cloud	Empfängt und aktualisiert Ergebnisse	Nicht zutreffend
Atlassian – Opsgenie	Erhält Ergebnisse	Nicht zutreffend
Fortinet – FortiCNP	Erhält Ergebnisse	Nicht zutreffend
IBM – QRadar	Erhält Ergebnisse	Nicht zutreffend

Integration	Richtung	ARN (falls zutreffend)
Logz.io Cloud SIEM	Erhält Ergebnisse	Nicht zutreffend
MetricStream	Erhält Ergebnisse	Nicht zutreffend
MicroFocus – MicroFocus Arcsight	Erhält Ergebnisse	Nicht zutreffend
New Relic Vulnerability Management	Erhält Ergebnisse	Nicht zutreffend
PagerDuty – PagerDuty	Erhält Ergebnisse	Nicht zutreffend
Palo Alto Networks – Cortex XSOAR	Erhält Ergebnisse	Nicht zutreffend
Palo Alto Networks – VM-Series	Erhält Ergebnisse	Nicht zutreffend
Rackspace Technology – Cloud Native Security	Erhält Ergebnisse	Nicht zutreffend
Rapid7 – InsightConnect	Erhält Ergebnisse	Nicht zutreffend
RSA – RSA Archer	Erhält Ergebnisse	Nicht zutreffend
ServiceNow – ITSM	Empfängt und aktualisiert Ergebnisse	Nicht zutreffend
Slack – Slack	Erhält Ergebnisse	Nicht zutreffend
Splunk – Splunk Enterprise	Erhält Ergebnisse	Nicht zutreffend
Splunk – Splunk Phantom	Erhält Ergebnisse	Nicht zutreffend
ThreatModeler	Erhält Ergebnisse	Nicht zutreffend
Trellix – Trellix Helix	Erhält Ergebnisse	Nicht zutreffend

Integration	Richtung	ARN (falls zutreffend)
Caveonix – Caveonix Cloud	Sendet und empfängt Ergebnisse	`arn:aws:securityhub: <REGION>::product/caveonix/caveonix-cloud`
Cloud Custodian – Cloud Custodian	Sendet und empfängt Ergebnisse	`arn:aws:securityhub: <REGION>::product/cloud-custodian/cloud-custodian`
DisruptOps, Inc. – DisruptOPS	Sendet und empfängt Ergebnisse	`arn:aws:securityhub: <REGION>::product/disruptops-inc/disruptops`
Kion	Sendet und empfängt Ergebnisse	`arn:aws:securityhub: <REGION>::product/cloudtamerio/cloudtamerio`
Turbot – Turbot	Sendet und empfängt Ergebnisse	`arn:aws:securityhub: <REGION>:453761072151:product/turbot/turbot`

Integrationen von Drittanbietern, die Ergebnisse an Security Hub senden

Die folgenden Produktintegrationen von Drittanbietern senden Ergebnisse an Security Hub. Security Hub wandelt die Ergebnisse in das AWS Security Finding Format um.

3CORESec – 3CORESec NTA

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/3coresec/3coresec`

3CORESecbietet verwaltete Erkennungsdienste sowohl für lokale Umgebungen als auch für AWS Systeme. Ihre Integration mit Security Hub ermöglicht Einblicke in Bedrohungen wie Malware, Rechteausweitung, laterale Bewegungen und unsachgemäße Netzwerksegmentierung.

Link zum Produkt

Dokumentation für Partner

Alert Logic – SIEMless Threat Management

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

Sorgen Sie für das richtige Maß an Schutz: Sichtbarkeit von Schwachstellen und Ressourcen, Bedrohungserkennung und Vorfallmanagement sowie zugewiesene SOC-Analystenoptionen. AWS WAF

Link zum Produkt

Dokumentation für Partner

Aqua Security – Aqua Cloud Native Security Platform

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP)bietet Sicherheit über den gesamten Lebenszyklus von containerbasierten und serverlosen Anwendungen, von Ihrer CI/CD-Pipeline bis hin zu Runtime-Produktionsumgebungen.

Link zum Produkt

Dokumentation für Partner

Aqua Security – Kube-bench

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-benchist ein Open-Source-Tool, das den Kubernetes-Benchmark des Center for Internet Security (CIS) in Ihrer Umgebung ausführt.

Link zum Produkt

Dokumentation für Partner

Armor – Armor Anywhere

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywherebietet verwaltete Sicherheit und Compliance für AWS.

Link zum Produkt

Dokumentation für Partner

AttackIQ – AttackIQ

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platformemuliert echtes gegnerisches Verhalten im Einklang mit dem MITRE ATT&CK Framework, um Ihre allgemeine Sicherheitslage zu validieren und zu verbessern.

Link zum Produkt

Dokumentation für Partner

Barracuda Networks – Cloud Security Guardian

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentryhilft Unternehmen dabei, beim Erstellen von Anwendungen in der Public Cloud und beim Verschieben von Workloads in die Public Cloud sicher zu bleiben.

AWS Link zum Marketplace

Link zum Produkt

BigID – BigID Enterprise

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

Das BigID Enterprise Privacy Management Platform hilft Unternehmen dabei, sensible Daten (PII) in all ihren Systemen zu verwalten und zu schützen.

Link zum Produkt

Dokumentation für Partner

Blue Hexagon— Blue Hexagon für AWS

Art der Integration: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagonist eine Plattform zur Erkennung von Bedrohungen in Echtzeit. Sie verwendet Deep-Learning-Prinzipien, um bekannte und unbekannte Bedrohungen, einschließlich Malware und Netzwerkanomalien, zu erkennen.

AWS Link zum Marketplace

Dokumentation für Partner

Capitis Solutions – C2VS

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/capitis/c2vs`

C2VSist eine anpassbare Compliance-Lösung, die entwickelt wurde, um Ihre anwendungsspezifischen Fehlkonfigurationen und deren Ursache automatisch zu identifizieren.

Link zum Produkt

Dokumentation für Partner

Check Point – CloudGuard IaaS

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuarderweitert auf einfache Weise die umfassende Sicherheit zur Bedrohungsabwehr AWS und schützt gleichzeitig Ressourcen in der Cloud.

Link zum Produkt

Dokumentation für Partner

Check Point – CloudGuard Posture Management

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

Eine SaaS-Plattform, die überprüfbare Cloud-Netzwerksicherheit, fortschrittlichen IAM-Schutz sowie umfassende Compliance und Governance bietet.

Link zum Produkt

Dokumentation für Partner

Claroty – xDome

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDomehilft Unternehmen dabei, ihre cyberphysischen Systeme im erweiterten Internet der Dinge (XIoT) in industriellen (OT), Gesundheits- (IoMT) und Unternehmensumgebungen (IoT) zu schützen.

Link zum Produkt

Dokumentation für Partner

Cloud Storage Security— Antivirus for Amazon S3

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Securitybietet Cloud-native Anti-Malware- und Antivirenscans für Amazon S3 S3-Objekte.

Antivirus for Amazon S3 bietet Echtzeit- und geplante Scans von Objekten und Dateien in Amazon S3 auf Malware und Bedrohungen. Es bietet Transparenz und Problembehebung bei problematischen und infizierten Dateien.

Link zum Produkt

Dokumentation für Partner

Contrast Security – Contrast Assess

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assessist ein IAST-Tool, das die Erkennung von Sicherheitslücken in Web-Apps, APIs und Microservices in Echtzeit ermöglicht. Contrast Assesslässt sich in Security Hub integrieren, um zentrale Transparenz und Reaktionsfähigkeit für all Ihre Workloads zu gewährleisten.

Link zum Produkt

Dokumentation für Partner

CrowdStrike – CrowdStrike Falcon

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

Der CrowdStrike Falcon einzelne, leichte Sensor vereint Virenschutz der nächsten Generation, Endpunkterkennung und -abwehr sowie eine rund um die Uhr verwaltete Suche in der Cloud.

Link zum Produkt

Dokumentation für Partner

CyberArk – Privileged Threat Analytics

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat AnalyticsErfassung, Erkennung und Reaktion auf risikoreiche Aktivitäten und Verhaltensweisen privilegierter Konten, um laufende Angriffe einzudämmen.

Link zum Produkt

Dokumentation für Partner

Data Theorem – Data Theorem

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theoremscannt kontinuierlich Webanwendungen, APIs und Cloud-Ressourcen auf der Suche nach Sicherheitslücken und Datenschutzlücken, um AppSec Datenschutzverletzungen zu verhindern.

Link zum Produkt

Dokumentation für Partner

Drata

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drataist eine Plattform zur Compliance-Automatisierung, mit der Sie die Einhaltung verschiedener Frameworks wie SOC2, ISO und GDPR erreichen und aufrechterhalten können. Die Integration zwischen Drata und Security Hub hilft Ihnen, Ihre Sicherheitserkenntnisse an einem Ort zu zentralisieren.

AWS Link zum Marketplace

Dokumentation für Partner

Forcepoint – Forcepoint CASB

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASBermöglicht es Ihnen, die Nutzung von Cloud-Anwendungen zu ermitteln, Risiken zu analysieren und angemessene Kontrollen für SaaS- und benutzerdefinierte Anwendungen durchzusetzen.

Link zum Produkt

Dokumentation für Partner

Forcepoint – Forcepoint Cloud Security Gateway

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gatewayist ein konvergenter Cloud-Sicherheitsdienst, der Transparenz, Kontrolle und Bedrohungsschutz für Benutzer und Daten bietet, unabhängig davon, wo sie sich befinden.

Link zum Produkt

Dokumentation für Partner

Forcepoint – Forcepoint DLP

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLPbegegnet Risiken, bei denen der Mensch im Mittelpunkt steht, und bietet Transparenz und Kontrolle überall dort, wo Ihre Mitarbeiter arbeiten und wo sich Ihre Daten befinden.

Link zum Produkt

Dokumentation für Partner

Forcepoint – Forcepoint NGFW

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFWermöglicht es Ihnen, Ihre AWS Umgebung mit Ihrem Unternehmensnetzwerk zu verbinden und bietet die Skalierbarkeit, den Schutz und die Einblicke, die Sie benötigen, um Ihr Netzwerk zu verwalten und auf Bedrohungen zu reagieren.

Link zum Produkt

Dokumentation für Partner

Fugue – Fugue

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugueist eine skalierbare Cloud-native Plattform ohne Agenten, die die kontinuierliche Validierung von Cloud-Laufzeitumgebungen automatisiert infrastructure-as-code und dabei dieselben Richtlinien verwendet.

Link zum Produkt

Dokumentation für Partner

Guardicore – Centra 4.0

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centrabietet Flussvisualisierung, Mikrosegmentierung und Erkennung von Sicherheitslücken für Workloads in modernen Rechenzentren und Clouds.

Link zum Produkt

Dokumentation für Partner

HackerOne – Vulnerability Intelligence

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

Die HackerOne Plattform arbeitet mit der weltweiten Hacker-Community zusammen, um die wichtigsten Sicherheitsprobleme aufzudecken. Vulnerability Intelligenceermöglicht es Ihrem Unternehmen, über automatisiertes Scannen hinauszugehen. Es enthält Sicherheitslücken, die von HackerOne ethischen Hackern validiert und Schritte zur Reproduktion bereitgestellt wurden.

AWS Link zum Marktplatz

Dokumentation für Partner

JFrog – Xray

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xrayist ein universelles Tool zur Analyse der Anwendungssicherheit (Software Composition Analysis, SCA), das Binärdateien kontinuierlich auf Lizenzbestimmungen und Sicherheitslücken scannt, sodass Sie eine sichere Software-Lieferkette betreiben können.

AWS Link zum Marketplace

Dokumentation für Partner

Juniper Networks – vSRX Next Generation Firewall

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks'vSRX Virtual Next Generation Firewall bietet eine vollständige cloudbasierte virtuelle Firewall mit erweiterter Sicherheit, sicherem SD-WAN, robustem Netzwerk und integrierter Automatisierung.

AWS Link zum Marketplace

Dokumentation für Partner

Link zum Produkt

k9 Security – Access Analyzer

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Securitybenachrichtigt Sie, wenn wichtige Zugangsänderungen in Ihrem AWS Identity and Access Management Konto vorgenommen werden. Damit können Sie nachvollziehenk9 Security, welchen Zugriff Benutzer und IAM-Rollen auf wichtige Daten AWS-Services und Ihre Daten haben.

k9 Securityist für Continuous Delivery konzipiert und ermöglicht es Ihnen, IAM mit umsetzbaren Zugriffsprüfungen und einfacher Richtlinienautomatisierung für und Terraform zu operationalisieren. AWS CDK

Link zum Produkt

Dokumentation für Partner

Lacework – Lacework

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Laceworkist die datengesteuerte Sicherheitsplattform für die Cloud. Die Lacework Cloud Security Platform automatisiert Cloud-Sicherheit in großem Maßstab, sodass Sie schnell und sicher innovieren können.

Link zum Produkt

Dokumentation für Partner

McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP)bietet Cloud Security Posture Management (CSPM) und Cloud Workload Protection Platform (CWPP) für Ihre Umgebung. AWS

Link zum Produkt

Dokumentation für Partner

NETSCOUT – NETSCOUT Cyber Investigator

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigatorist eine unternehmensweite Plattform für Netzwerkbedrohungen, Risikountersuchungen und forensische Analysen, die dazu beiträgt, die Auswirkungen von Cyberbedrohungen auf Unternehmen zu verringern.

Link zum Produkt

Dokumentation für Partner

Palo Alto Networks – Prisma Cloud Compute

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Computeist eine Cloud-native Cybersicherheitsplattform, die VMs, Container und serverlose Plattformen schützt.

Link zum Produkt

Dokumentation für Partner

Palo Alto Networks – Prisma Cloud Enterprise

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

Schützt Ihre AWS Bereitstellung mit Cloud-Sicherheitsanalysen, fortschrittlicher Bedrohungserkennung und Compliance-Überwachung.

Link zum Produkt

Dokumentation für Partner

Plerion – Cloud Security Platform

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerionist eine Cloud-Sicherheitsplattform mit einem einzigartigen, bedrohungsorientierten, risikoorientierten Ansatz, der präventive, detektive und korrektive Maßnahmen für Ihre Workloads bietet. Die Integration zwischen Plerion und Security Hub ermöglicht es Kunden, ihre Sicherheitsergebnisse an einem Ort zu zentralisieren und entsprechend zu handeln.

AWS Link zum Marketplace

Dokumentation für Partner

Prowler – Prowler

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowlerist ein Open-Source-Sicherheitstool zur Durchführung von AWS Prüfungen in Bezug auf bewährte Sicherheitsverfahren, Abhärtung und kontinuierliche Überwachung.

Link zum Produkt

Dokumentation für Partner

Qualys – Vulnerability Management

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM)scannt und identifiziert kontinuierlich Sicherheitslücken und schützt so Ihre Ressourcen.

Link zum Produkt

Dokumentation für Partner

Rapid7 – InsightVM

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVM bietet Schwachstellenmanagement für moderne Umgebungen, sodass Sie Sicherheitslücken effizient finden, priorisieren und beheben können.

Link zum Produkt

Dokumentation für Partner

SecureCloudDB – SecureCloudDB

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/securecloudd b/securecloudd b`

SecureCloudDBist ein Cloud-natives Datenbanksicherheitstool, das einen umfassenden Überblick über interne und externe Sicherheitslage und -aktivitäten bietet. Es kennzeichnet Sicherheitsverletzungen und behebt ausnutzbare Datenbankschwachstellen.

Link zum Produkt

Dokumentation für Partner

SentinelOne – SentinelOne

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOneist eine autonome XDR-Plattform (Extended Detection and Response), die KI-gestützte Prävention, Erkennung, Reaktion und Suche über Endpunkte, Container, Cloud-Workloads und IoT-Geräte hinweg umfasst.

AWS Link zum Marketplace

Link zum Produkt

Snyk

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snykbietet eine Sicherheitsplattform, die App-Komponenten auf Sicherheitsrisiken in Workloads überprüft, auf AWS denen sie ausgeführt werden. Diese Risiken werden als Ergebnisse an Security Hub gesendet, sodass Entwickler und Sicherheitsteams sie zusammen mit den übrigen AWS Sicherheitsergebnissen visualisieren und priorisieren können.

AWS Link zum Marketplace

Dokumentation für Partner

Sonrai Security – Sonrai Dig

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Digüberwacht und behebt Cloud-Fehlkonfigurationen und Richtlinienverstöße, sodass Sie Ihren Sicherheits- und Compliance-Status verbessern können.

Link zum Produkt

Dokumentation für Partner

Sophos – Server Protection

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protectionschützt die kritischen Anwendungen und Daten, die das Herzstück Ihres Unternehmens bilden, mithilfe umfassender defense-in-depth Techniken.

Link zum Produkt

Dokumentation für Partner

StackRox – StackRox Kubernetes Security

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRoxhilft Unternehmen dabei, ihre Container- und Kubernetes-Implementierungen in großem Umfang zu sichern, indem sie ihre Compliance- und Sicherheitsrichtlinien über den gesamten Container-Lebenszyklus hinweg durchsetzen — bei der Erstellung, Bereitstellung und Ausführung.

Link zum Produkt

Dokumentation für Partner

Sumo Logic – Machine Data Analytics

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logicist eine sichere Plattform zur Analyse von Maschinendaten, mit der Entwicklungs- und Sicherheitsteams ihre AWS Anwendungen erstellen, ausführen und sichern können.

Link zum Produkt

Dokumentation für Partner

Symantec – Cloud Workload Protection

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protectionbietet umfassenden Schutz für Ihre Amazon EC2 EC2-Instances mit Malware-Schutz, Intrusion Prevention und Überwachung der Dateiintegrität.

Link zum Produkt

Dokumentation für Partner

Tenable – Tenable.io

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

Präzises Identifizieren, Untersuchen und Priorisieren von Schwachstellen. In der Cloud verwaltet.

Link zum Produkt

Dokumentation für Partner

Trend Micro – Cloud One

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud Onestellt Teams zur richtigen Zeit und am richtigen Ort die richtigen Sicherheitsinformationen zur Verfügung. Diese Integration sendet Sicherheitsergebnisse in Echtzeit an Security Hub und verbessert so die Sichtbarkeit Ihrer AWS Ressourcen und Trend Micro Cloud One Ereignisdetails in Security Hub.

AWS Link zum Marketplace

Dokumentation für Partner

Vectra – Cognito Detect

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectraverändert die Cybersicherheit, indem es fortschrittliche KI einsetzt, um versteckte Cyberangreifer zu erkennen und darauf zu reagieren, bevor sie stehlen oder Schaden anrichten können.

AWS Link zum Marketplace

Dokumentation für Partner

Wiz – Wiz Security

Integrationstyp: Senden

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wizanalysiert kontinuierlich Konfigurationen, Sicherheitslücken, Netzwerke, IAM-Einstellungen, Geheimnisse und mehr für Ihre AWS-Konten Benutzer und Workloads, um kritische Probleme zu entdecken, die ein echtes Risiko darstellen. Integrieren Sie Wiz in Security Hub, um Probleme zu visualisieren und darauf zu reagieren, die Wiz von der Security Hub Hub-Konsole aus erkennt.

AWS Link zum Marketplace

Dokumentation für Partner

Integrationen von Drittanbietern, die Erkenntnisse von Security Hub erhalten

Die folgenden Produktintegrationen von Drittanbietern stammen von Security Hub. Sofern angegeben, können die Produkte die Ergebnisse auch aktualisieren. In diesem Fall wird das Auffinden von Updates, die Sie im Partnerprodukt vornehmen, auch in Security Hub widergespiegelt.

Atlassian - Jira Service Management

Integrationstyp: Empfangen und aktualisieren

Das AWS Service Management Connector for Jira sendet Ergebnisse von Security Hub anJira. JiraProbleme werden auf der Grundlage der Ergebnisse erstellt. Wenn die Jira Probleme aktualisiert werden, werden die entsprechenden Ergebnisse in Security Hub aktualisiert.

Die Integration unterstützt nur Jira Server und Jira Data Center.

Einen Überblick über die Integration und ihre Funktionsweise finden Sie im Video AWS Security Hub — Bidirektionale Integration mit Atlassian Jira Service Management.

Link zum Produkt

Dokumentation für Partner

Atlassian - Jira Service Management Cloud

Integrationstyp: Empfangen und aktualisieren

Jira Service Management Cloudist die Cloud-Komponente von Jira Service Management.

Das AWS Service Management Connector for Jira sendet Ergebnisse von Security Hub anJira. Die Ergebnisse lösen die Entstehung von Problemen in ausJira Service Management Cloud. Wenn Sie diese Probleme in aktualisierenJira Service Management Cloud, werden die entsprechenden Ergebnisse auch in Security Hub aktualisiert.

Link zum Produkt

Dokumentation für Partner

Atlassian – Opsgenie

Integrationstyp: Empfangen

Opsgenieist eine moderne Incident-Management-Lösung für den Betrieb ständig verfügbarer Dienste, die es Entwicklungs- und Betriebsteams ermöglicht, Serviceunterbrechungen zu planen und bei Vorfällen die Kontrolle zu behalten.

Durch die Integration mit Security Hub wird sichergestellt, dass geschäftskritische sicherheitsrelevante Vorfälle zur sofortigen Lösung an die entsprechenden Teams weitergeleitet werden.

Link zum Produkt

Dokumentation für Partner

Fortinet – FortiCNP

Integrationstyp: Empfangen

FortiCNPist ein Cloud-Native-Protection-Produkt, das Sicherheitserkenntnisse zu umsetzbaren Erkenntnissen zusammenfasst und Sicherheitsinformationen auf der Grundlage der Risikobewertung priorisiert, um Alarmermüdung zu reduzieren und Problembehebungen zu beschleunigen.

AWS Link zum Marketplace

Dokumentation für Partner

IBM – QRadar

Integrationstyp: Empfangen

IBM QRadarSIEM bietet Sicherheitsteams die Möglichkeit, Bedrohungen schnell und präzise zu erkennen, zu priorisieren, zu untersuchen und darauf zu reagieren.

Link zum Produkt

Dokumentation für Partner

Logz.io Cloud SIEM

Integrationstyp: Empfangen

Logz.ioist ein AnbieterCloud SIEM, der eine erweiterte Korrelation von Protokoll- und Ereignisdaten bereitstellt, um Sicherheitsteams dabei zu unterstützen, Sicherheitsbedrohungen in Echtzeit zu erkennen, zu analysieren und darauf zu reagieren.

Link zum Produkt

Dokumentation für Partner

MetricStream – CyberGRC

Integrationstyp: Empfangen

MetricStream CyberGRChilft Ihnen bei der Verwaltung, Messung und Minderung von Cybersicherheitsrisiken. Durch den Empfang der Ergebnisse von Security Hub erhalten Sie CyberGRC einen besseren Einblick in diese Risiken, sodass Sie Investitionen in die Cybersicherheit priorisieren und IT-Richtlinien einhalten können.

AWS Link zum Marketplace

Link zum Produkt

MicroFocus – MicroFocus Arcsight

Integrationstyp: Empfangen

ArcSightbeschleunigt die effektive Erkennung und Reaktion auf Bedrohungen in Echtzeit und integriert dabei die Korrelation von Ereignissen sowie überwachte und unbeaufsichtigte Analysen mit der Automatisierung und Orchestrierung von Reaktionen.

Link zum Produkt

Dokumentation für Partner

New Relic Vulnerability Management

Integrationstyp: Empfangen

New Relic Vulnerability Managementempfängt Sicherheitsergebnisse von Security Hub, sodass Sie einen zentralen Überblick über die Sicherheit und die Leistungstelemetrie im Kontext Ihres gesamten Stacks erhalten.

AWS Link zum Marketplace

Dokumentation für Partner

PagerDuty – PagerDuty

Integrationstyp: Empfangen

Die PagerDuty digitale Betriebsmanagement-Plattform ermöglicht es Teams, proaktiv Probleme zu lösen, die sich auf Kunden auswirken, indem jedes Signal automatisch in die richtigen Erkenntnisse und Maßnahmen umgewandelt wird.

AWS Benutzer können die PagerDuty Reihe von AWS Integrationen nutzen, um ihre AWS und hybride Umgebungen vertrauensvoll zu skalieren.

In Kombination mit aggregierten und organisierten Sicherheitswarnungen von Security Hub PagerDuty können Teams ihren Prozess zur Reaktion auf Bedrohungen automatisieren und schnell benutzerdefinierte Aktionen einrichten, um potenziellen Problemen vorzubeugen.

PagerDutyBenutzer, die ein Cloud-Migrationsprojekt durchführen, können schnell handeln und gleichzeitig die Auswirkungen von Problemen verringern, die während des Migrationszyklus auftreten.

Link zum Produkt

Dokumentation für Partner

Palo Alto Networks – Cortex XSOAR

Integrationstyp: Empfangen

Cortex XSOARist eine SOAR-Plattform (Security Orchestration, Automation and Response), die sich in Ihr gesamtes Sicherheitsprodukteportfolio integrieren lässt, um die Reaktion auf Vorfälle und die Sicherheitsabläufe zu beschleunigen.

Link zum Produkt

Dokumentation für Partner

Palo Alto Networks – VM-Series

Integrationstyp: Empfangen

Palo Alto VM-SeriesDie Integration mit Security Hub sammelt Bedrohungsinformationen und sendet sie als automatisches Update der Sicherheitsrichtlinien an die Firewall der VM-Series nächsten Generation, das böswillige IP-Adressaktivitäten blockiert.

Link zum Produkt

Dokumentation für Partner

Rackspace Technology – Cloud Native Security

Integrationstyp: Empfangen

Rackspace Technology bietet zusätzlich zu systemeigenen Sicherheitsprodukten verwaltete AWS Sicherheitsdienste für die Überwachung rund um die Uhr durch Rackspace SOC, erweiterte Analysen und die Beseitigung von Bedrohungen.

Link zum Produkt

Rapid7 – InsightConnect

Integrationstyp: Empfangen

Rapid7 InsightConnectist eine Lösung zur Sicherheitsorchestrierung und Automatisierung, mit der Ihr Team den SOC-Betrieb mit wenig bis gar keinem Code optimieren kann.

Link zum Produkt

Dokumentation für Partner

RSA – RSA Archer

Integrationstyp: Empfangen

RSA ArcherMit IT- und Sicherheitsrisikomanagement können Sie ermitteln, welche Ressourcen für Ihr Unternehmen von entscheidender Bedeutung sind, Sicherheitsrichtlinien und -standards festlegen und kommunizieren, Angriffe erkennen und darauf reagieren, Sicherheitsmängel identifizieren und beheben sowie klare Best Practices für das IT-Risikomanagement festlegen.

Link zum Produkt

Dokumentation für Partner

ServiceNow – ITSM

Integrationstyp: Empfangen und aktualisieren

ServiceNowDurch die Integration mit Security Hub können die Sicherheitsergebnisse von Security Hub darin eingesehen werdenServiceNow ITSM. Sie können auch so konfigurierenServiceNow, dass automatisch ein Vorfall oder ein Problem erstellt wird, wenn es einen Befund von Security Hub erhält.

Alle Aktualisierungen dieser Vorfälle und Probleme führen zu Aktualisierungen der Ergebnisse in Security Hub.

Einen Überblick über die Integration und ihre Funktionsweise finden Sie im Video AWS Security Hub — Bidirektionale Integration mit ServiceNow ITSM.

Link zum Produkt

Dokumentation für Partner

Slack – Slack

Integrationstyp: Empfangen

Slackist eine Ebene des Technologie-Stacks für Unternehmen, die Menschen, Daten und Anwendungen zusammenbringt. Es ist ein zentraler Ort, an dem Menschen effektiv zusammenarbeiten, wichtige Informationen finden und auf Hunderttausende kritischer Anwendungen und Services zugreifen können, um Spitzenleistungen zu erbringen.

Link zum Produkt

Dokumentation für Partner

Splunk – Splunk Enterprise

Integrationstyp: Empfangen

Splunkverwendet Amazon CloudWatch Events als Nutzer von Security Hub Hub-Ergebnissen. Senden Sie Ihre Daten Splunk für erweiterte Sicherheitsanalysen und SIEM an.

Link zum Produkt

Dokumentation für Partner

Splunk – Splunk Phantom

Integrationstyp: Empfangen

Mit der Splunk Phantom Anwendung für AWS Security Hub werden die Ergebnisse Phantom zur automatisierten Kontextanreicherung mit zusätzlichen Bedrohungsinformationen oder zur Durchführung automatisierter Reaktionsmaßnahmen gesendet.

Link zum Produkt

Dokumentation für Partner

ThreatModeler

Integrationstyp: Empfangen

ThreatModelerist eine automatisierte Lösung zur Bedrohungsmodellierung, die den Lebenszyklus von Unternehmenssoftware und Cloud-Entwicklung schützt und skaliert.

Link zum Produkt

Dokumentation für Partner

Trellix – Trellix Helix

Integrationstyp: Empfangen

Trellix Helixist eine in der Cloud gehostete Plattform für Sicherheitsoperationen, die es Unternehmen ermöglicht, die Kontrolle über jeden Vorfall von der Warnung bis zur Behebung zu übernehmen.

Link zum Produkt

Dokumentation für Partner

Integrationen von Drittanbietern, die Ergebnisse an Security Hub senden und Ergebnisse von Security Hub empfangen

Die folgenden Produktintegrationen von Drittanbietern senden Ergebnisse an Security Hub und empfangen Ergebnisse von Security Hub.

Caveonix – Caveonix Cloud

Integrationstyp: Senden und Empfangen

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

Die Caveonix KI-gestützte Plattform automatisiert Transparenz, Bewertung und Risikominderung in Hybrid-Clouds und deckt Cloud-native Dienste, VMs und Container ab. Integriert in AWS Security Hub, Caveonix führt AWS Daten und erweiterte Analysen zusammen, um Einblicke in Sicherheitswarnungen und Compliance zu erhalten.

AWS Link zum Marketplace

Dokumentation für Partner

Cloud Custodian – Cloud Custodian

Integrationstyp: Senden und Empfangen

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodianermöglicht es Benutzern, in der Cloud gut verwaltet zu werden. Das einfache YAML-DSL ermöglicht einfach zu definierende Regeln, um eine gut verwaltete Cloud-Infrastruktur zu ermöglichen, die sowohl sicher als auch kostenoptimiert ist.

Link zum Produkt

Dokumentation für Partner

DisruptOps, Inc. – DisruptOPS

Integrationstyp: Senden und Empfangen

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

Die DisruptOps Security Operations Platform unterstützt Unternehmen dabei, mithilfe automatisierter Leitplanken die besten Sicherheitspraktiken in Ihrer Cloud aufrechtzuerhalten.

Link zum Produkt

Dokumentation für Partner

Kion

Integrationstyp: Senden und Empfangen

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion(ehemals cloudtamer.io) ist eine komplette Cloud-Governance-Lösung für. AWSKionbietet Stakeholdern Einblick in den Cloud-Betrieb und hilft Cloud-Nutzern dabei, Konten zu verwalten, Budget und Kosten zu kontrollieren und die kontinuierliche Einhaltung von Vorschriften sicherzustellen.

Link zum Produkt

Dokumentation für Partner

Turbot – Turbot

Integrationstyp: Senden und Empfangen

Produkt-ARN: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbotstellt sicher, dass Ihre Cloud-Infrastruktur sicher, konform, skalierbar und kostenoptimiert ist.

Link zum Produkt

Dokumentation für Partner

Verwenden von benutzerdefinierten Produktintegrationen, um Ergebnisse an AWS Security Hub zu senden

Zusätzlich zu den Ergebnissen, die durch die integrierten AWS Dienste und Produkte von Drittanbietern generiert wurden, kann Security Hub auch Ergebnisse verwenden, die von anderen kundenspezifischen Sicherheitsprodukten generiert wurden.

Sie können diese Ergebnisse mithilfe der `BatchImportFindings`API-Operation manuell an Security Hub senden.

Verwenden Sie bei der Einrichtung der benutzerdefinierten Integration die Richtlinien und Checklisten im Security Hub Partner Integration Guide.

Anforderungen und Empfehlungen für das Senden von Ergebnissen aus benutzerdefinierten Sicherheitsprodukten

Bevor Sie den `BatchImportFindings`API-Vorgang erfolgreich aufrufen können, müssen Sie Security Hub aktivieren.

Sie müssen die Ergebnisdetails mit dem the section called “Ergebnisformat” angeben. Verwenden Sie für die Ergebnisse Ihrer benutzerdefinierten Integration die folgenden Anforderungen und Empfehlungen.

Einstellen des Produkt-ARNs

Wenn Sie Security Hub aktivieren, wird ein Standardprodukt Amazon Resource Name (ARN) für Security Hub in Ihrem aktuellen Konto generiert.

Dieser Produkt-ARN weist das folgende Format auf: `arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default`. z. B. `arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default`.

Verwenden Sie diesen Produkt-ARN als Wert für das `ProductArn`-Attribut, wenn Sie die `BatchImportFindings`-API-Operation aufrufen.

Definition des Unternehmens- und Produktnamens

Sie können `BatchImportFindings` damit einen bevorzugten Firmen- und Produktnamen für die benutzerdefinierte Integration festlegen, die Ergebnisse an Security Hub sendet.

Ihre angegebenen Namen ersetzen den vorkonfigurierten Firmennamen und den Produktnamen, genannt persönlicher Name bzw. Standardname, und werden in der Security Hub Hub-Konsole und im JSON jedes Fundes angezeigt. Siehe Verwenden von BatchImportFindings zum Erstellen und Aktualisieren von Ergebnissen.

Einstellen der Ergebnis-IDs

Sie müssen Ihre eigenen Ergebnis-IDs mit dem `Id`-Attribut bereitstellen, verwalten und inkrementieren.

Jeder neue Befund sollte eine eindeutige Ergebnis-ID haben. Wenn das benutzerdefinierte Produkt mehrere Ergebnisse mit derselben Befund-ID sendet, verarbeitet Security Hub nur den ersten Befund.

Einstellen der Konto-ID

Sie müssen mit dem `AwsAccountId`-Attribut Ihre eigene Konto-ID angeben.

Einstellen Erstellungs- und Aktualisierungsdatums

Sie müssen eigene Zeitstempel für die Attribute `CreatedAt` und `UpdatedAt` angeben.

Importieren von Ergebnissen aus benutzerdefinierten Produkten

Zusätzlich zum Senden neuer Ergebnisse aus benutzerdefinierten Produkten können Sie auch die `BatchImportFindings`-API-Operation verwenden, um vorhandene Ergebnisse aus benutzerdefinierten Produkten zu aktualisieren.

Um vorhandene Ergebnisse zu aktualisieren, verwenden Sie die vorhandene Ergebnis-ID (über das `Id`-Attribut). Senden Sie das vollständige Ergebnis erneut mit den entsprechenden Informationen, die in der Anforderung aktualisiert wurden, einschließlich eines geänderten `UpdatedAt`-Zeitstempels.

Beispiel für benutzerdefinierte Integrationen

Sie können das folgende Beispiel für benutzerdefinierte Produktintegrationen als Leitfaden verwenden, um Ihre eigene benutzerdefinierte Lösung zu erstellen.

Ergebnisse von Chef InSpec Scans an Security Hub senden

Sie können eine AWS CloudFormation Vorlage erstellen, die einen Chef InSpec Konformitätsscan durchführt und die Ergebnisse dann an Security Hub sendet.

Weitere Informationen finden Sie unter Kontinuierliche Compliance-Überwachung mit Chef InSpec und AWS Security Hub.

Von entdeckte Container-Schwachstellen Trivy an Security Hub senden

Sie können eine AWS CloudFormation Vorlage erstellen, mit der Container AquaSecurity Trivy nach Sicherheitslücken gescannt werden, und die gefundenen Sicherheitslücken dann an Security Hub gesendet werden.

Weitere Informationen finden Sie unter So erstellen Sie eine CI/CD-Pipeline für das Scannen von Container-Schwachstellen mit Trivy und AWS Security Hub.

Sicherheitskontrollen und -standards in AWS Security Hub

AWS Security Hub nutzt, aggregiert und analysiert Sicherheitsergebnisse verschiedener unterstützter Produkte AWS und Produkte von Drittanbietern.

Security Hub generiert auch seine eigenen Ergebnisse, indem es automatisierte und kontinuierliche Sicherheitsprüfungen anhand von Regeln durchführt. Die Regeln werden durch Sicherheitskontrollen repräsentiert. Die Kontrollen können wiederum in einem oder mehreren Sicherheitsstandards aktiviert werden. Mithilfe der Kontrollen können Sie feststellen, ob die Anforderungen eines Standards erfüllt werden.

Sicherheitsprüfungen anhand von Kontrollen führen zu Ergebnissen, anhand derer Sie Ihren Sicherheitsstatus überwachen und bestimmte Ressourcen AWS-Konten oder Ressourcen identifizieren können, die Ihrer Aufmerksamkeit bedürfen. Jede Kontrolle bezieht sich auf einen AWS Dienst und eine Ressource. Beispielsweise wird anhand von Sicherheitsprüfungen anhand des CloudTrail2.4-Steuerelements ermittelt, ob Sie die Überprüfung der Protokolldateien für Ihre AWS CloudTrail Protokolle konfiguriert haben. Weitere Informationen zu Steuerelementen finden Sie unterSicherheitskontrollen anzeigen und verwalten.

Sie können ein Steuerelement in einem oder mehreren aktivierten Security Hub Hub-Standards aktivieren. Wenn Sie einen Standard aktivieren, aktiviert Security Hub automatisch die Kontrollen, die für den Standard gelten. Sicherheitsstandards ermöglichen es Ihnen, sich auf ein bestimmtes Compliance-Framework zu konzentrieren. Security Hub definiert die Kontrollen, die für jeden Standard gelten. Weitere Informationen zu Sicherheitsstandards finden Sie unterSicherheitsstandards anzeigen und verwalten.

Auf der Grundlage der Ergebnisse von Sicherheitsprüfungen berechnet Security Hub eine allgemeine Sicherheitsbewertung und standardspezifische Sicherheitsbewertungen. Diese Bewertungen helfen Ihnen dabei, Ihren Sicherheitsstatus zu verstehen. Weitere Informationen zu Punktzahlen finden Sie unterWie werden Sicherheitswerte berechnet.

Informationen zu den Security Hub Hub-Preisen für Sicherheitsüberprüfungen finden Sie unter Security Hub Hub-Preise.

Themen

- Sicherheitsstandards anzeigen und verwalten
- Referenz zu Security Hub-Steuerungen
- Sicherheitskontrollen anzeigen und verwalten

IAM-Berechtigungen zur Konfiguration von Standards und Kontrollen

Um Informationen über Sicherheitskontrollen anzuzeigen und Sicherheitskontrollen in Standards zu aktivieren und zu deaktivieren, AWS Security Hub benötigt die AWS Identity and Access Management (IAM) -Rolle, die Sie für den Zugriff verwenden, Berechtigungen zum Aufrufen der folgenden API-Aktionen. Ohne das Hinzufügen von Berechtigungen für diese Aktionen können Sie diese APIs nicht aufrufen. Um die erforderlichen Berechtigungen zu erhalten, können Sie verwaltete Security Hub Hub-Richtlinien verwenden. Alternativ können Sie benutzerdefinierte IAM-Richtlinien so aktualisieren, dass sie Berechtigungen für diese Aktionen enthalten. Benutzerdefinierte Richtlinien sollten auch Berechtigungen für die `UpdateStandardsControl`APIs `DescribeStandardsControls`und enthalten.

- **`BatchGetSecurityControls`**— Gibt Informationen über eine Reihe von Sicherheitskontrollen für das Girokonto zurück und AWS-Region.
- **`ListSecurityControlDefinitions`**— Gibt Informationen über Sicherheitskontrollen zurück, die für einen bestimmten Standard gelten.
- **`ListStandardsControlAssociations`**— Identifiziert, ob eine Sicherheitskontrolle derzeit in jedem aktivierten Standard im Konto aktiviert oder deaktiviert ist.
- **`BatchGetStandardsControlAssociations`**— Identifiziert für eine Reihe von Sicherheitskontrollen, ob die einzelnen Kontrollen derzeit in einem bestimmten Standard aktiviert oder deaktiviert sind.
- **`BatchUpdateStandardsControlAssociations`**— Wird verwendet, um eine Sicherheitskontrolle in Standards zu aktivieren, die die Steuerung enthalten, oder um eine Steuerung in Standards zu deaktivieren. Dies ist ein Batch-Ersatz für die bestehende `UpdateStandardsControl`API, wenn ein Administrator nicht möchte, dass Mitgliedskonten Kontrollen aktivieren oder deaktivieren.

Zusätzlich zu den oben genannten APIs sollten Sie Ihrer IAM-Rolle die Berechtigung **`BatchGetControlEvaluations`**zum Aufrufen hinzufügen. Diese Berechtigung ist erforderlich, um den Aktivierungs- und Konformitätsstatus einer Kontrolle, die Ergebnisse für eine Kontrolle und

die Gesamtsicherheitsbewertung für Kontrollen auf der Security Hub Hub-Konsole einzusehen. Da nur die Konsole aufruft **`BatchGetControlEvaluations`**, entspricht diese IAM-Berechtigung nicht direkt den öffentlich dokumentierten Security Hub Hub-APIs oder AWS CLI -Befehlen.

Weitere Informationen zu APIs im Zusammenhang mit Kontrollen und Standards finden Sie in der AWS Security Hub API-Referenz.

Sicherheitsüberprüfungen und Sicherheitsbewertungen in Security Hub

AWS Security Hub Führt für jedes Steuerelement, das Sie aktivieren, Sicherheitsüberprüfungen durch. Bei einer Sicherheitsüberprüfung wird festgestellt, ob Ihre AWS Ressourcen den Regeln entsprechen, die das Steuerelement beinhaltet.

Einige Prüfungen werden in regelmäßigen Abständen ausgeführt. Andere Prüfungen werden nur ausgeführt, wenn sich der Ressourcenstatus ändert. Weitere Informationen finden Sie unter the section called “Zeitplan für die Ausführung von Sicherheitsprüfungen”.

Viele Sicherheitsüberprüfungen verwenden AWS Config verwaltete oder benutzerdefinierte Regeln, um die Konformitätsanforderungen festzulegen. Um diese Prüfungen ausführen zu können, müssen Sie sie einrichten AWS Config. Weitere Informationen finden Sie unter the section called “AWS Config Regeln und Sicherheitsüberprüfungen”. Andere verwenden benutzerdefinierte Lambda-Funktionen, die von Security Hub verwaltet werden und für Kunden nicht sichtbar sind.

Bei der Durchführung von Sicherheitsprüfungen generiert Security Hub Ergebnisse und weist ihnen einen Compliance-Status zu. Weitere Informationen zum Compliance-Status finden Sie unterWerte für den Konformitätsstatus eines Ergebnisses.

Security Hub verwendet den Compliance-Status der Kontrollergebnisse, um einen allgemeinen Kontrollstatus zu ermitteln. Security Hub berechnet außerdem eine Sicherheitsbewertung für alle aktivierten Kontrollen und für bestimmte Standards. Weitere Informationen finden Sie unter the section called “Konformitätsstatus und Kontrollstatus” und the section called “Ermittlung von Sicherheitseinstufungen”.

Wenn Sie konsolidierte Kontrollergebnisse aktiviert haben, generiert Security Hub ein einzelnes Ergebnis, auch wenn eine Kontrolle mit mehr als einem Standard verknüpft ist. Weitere Informationen finden Sie unter Konsolidierte Kontrollergebnisse.

Themen

So verwendet Security Hub AWS Config Regeln zur Durchführung von Sicherheitsüberprüfungen

Um Sicherheitsüberprüfungen für die Ressourcen Ihrer Umgebung durchzuführen, verwenden Sie AWS Security Hub entweder die im Standard angegebenen Schritte oder spezielle AWS Config Regeln. Bei einigen Regeln handelt es sich um verwaltete Regeln, die von verwaltet werden AWS Config. Andere Regeln sind benutzerdefinierte Regeln, die Security Hub entwickelt.

AWS Config Regeln, die Security Hub für Kontrollen verwendet, werden als dienstbezogene Regeln bezeichnet, da sie vom Security Hub Hub-Dienst aktiviert und gesteuert werden.

Um Prüfungen anhand dieser AWS Config Regeln zu aktivieren, müssen Sie zunächst die Aktivierung AWS Config für Ihr Konto und die Ressourcenaufzeichnung für die erforderlichen Ressourcen aktivieren. Informationen zur Aktivierung finden Sie AWS Config unterKonfiguration AWS Config. Hinweise zur erforderlichen Ressourcenaufzeichnung finden Sie unter AWS Config Ressourcen, die zur Generierung der Kontrollergebnisse erforderlich sind

So generiert Security Hub die serviceverknüpften Regeln

Für jedes Steuerelement, das eine AWS Config serviceverknüpfte Regel verwendet, erstellt Security Hub Instanzen der erforderlichen Regeln in Ihrer AWS Umgebung.

Diese dienstbezogenen Regeln sind spezifisch für Security Hub. Sie werden auch dann erstellt, wenn andere Instances derselben Regeln bereits vorhanden sind. Bei der serviceverknüpften Regel wird `securityhub` vor dem ursprünglichen Regelnamen und nach dem Regelnamen ein eindeutiger Bezeichner hinzugefügt. Für die ursprünglich AWS Config verwaltete Regel `vpc-flow-logs-enabled` würde der Name der serviceverknüpften Regel beispielsweise so lauten. `securityhub-vpc-flow-logs-enabled-12345`

Die Anzahl der AWS Config Regeln, die zur Auswertung von Kontrollen verwendet werden können, ist begrenzt. Benutzerdefinierte AWS Config Regeln, die Security Hub erstellt, werden nicht auf

dieses Limit angerechnet. Sie können einen Sicherheitsstandard aktivieren, auch wenn Sie das AWS Config Limit für verwaltete Regeln in Ihrem Konto bereits erreicht haben. Weitere Informationen zu AWS Config Regellimits finden Sie unter Service Limits im AWS Config Developer Guide.

Details zu den AWS Config Regeln für Kontrollen anzeigen

Bei Kontrollen, die AWS Config verwaltete Regeln verwenden, enthält die Beschreibung des Steuerelements einen Link zu den AWS Config Regeldetails. Benutzerdefinierte Regeln sind nicht mit der Beschreibung des Steuerelements verknüpft. Beschreibungen der Steuerelemente finden Sie unterReferenz zu Security Hub-Steuerungen. Wählen Sie ein Steuerelement aus der Liste aus, um dessen Beschreibung zu sehen.

Bei Ergebnissen, die anhand dieser Kontrollen generiert wurden, enthalten die Ergebnisdetails einen Link zu der zugehörigen AWS Config Regel. Beachten Sie, dass Sie im ausgewählten Konto auch über eine IAM-Berechtigung verfügen müssen, um von den Suchdetails zur AWS Config Regel zu AWS Config gelangen.

Die Ergebnisdetails auf den Seiten „Ergebnisse“, „Einblicke“ und „Integrationen“ enthalten einen Link „Regeln“ zu den AWS Config Regeldetails. Siehe Details zu den Ergebnissen werden überprüft.

Auf der Seite mit den Kontrolldetails enthält die Spalte Untersuchen der Ergebnisliste einen Link zu den AWS Config Regeldetails. Siehe Die AWS Config Regel für eine Suchressource anzeigen.

AWS Config Ressourcen, die zur Generierung der Kontrollergebnisse erforderlich sind

AWS Security Hub generiert Kontrollergebnisse, indem Sicherheitsprüfungen anhand der Security Hub Hub-Kontrollen durchgeführt werden. Bei einigen Kontrollen werden AWS Config Regeln verwendet, anhand derer die Einhaltung bestimmter Ressourcen bewertet wird. Damit Security Hub Ergebnisse für Kontrollen generieren kann, für die der Zeitplantyp „Änderung ausgelöst“ gilt, müssen Sie die Aufzeichnung für benötigte Ressourcen in aktivieren AWS Config. Für die meisten Kontrollen, die einen periodischen Zeitplan haben, müssen Sie keine Ressourcen aufzeichnen. Bei einigen regelmäßigen Kontrollen ist jedoch eine Erfassung von Ressourcen erforderlich, um Änderungen bei der Einhaltung von Vorschriften zu erkennen.

Diese Seite enthält eine Liste der erforderlichen Ressourcen für alle Standards sowie eine nach Standards aufgeschlüsselte Liste der erforderlichen Ressourcen. In der ersten Tabelle ist auch aufgeführt, welche Security Hub-Steuerelemente die einzelnen Ressourcen verwenden.

Wenn ein Ergebnis durch eine Sicherheitsüberprüfung generiert wird, die auf einer AWS Config Regel basiert, enthalten die Ergebnisdetails einen Link „Regeln“ zu der zugehörigen AWS Config Regel. Um zu der AWS Config Regel zu gelangen, muss Ihr Konto über IAM-Berechtigungen zum Anzeigen von AWS Config Regeln verfügen.

> **Note**
>
> AWS-Regionen Wenn ein Steuerelement nicht verfügbar ist, ist die entsprechende Ressource in AWS Config nicht verfügbar. Eine Liste der regionalen Beschränkungen für Security Hub-Steuerungen finden Sie unterVerfügbarkeit von Kontrollen nach Regionen.

AWS Config Ressourcen, die für alle Kontrollen erforderlich sind

Damit Security Hub Ergebnisse für aktivierte, von Security Hub Hub-Änderungen ausgelöste Kontrollen generiert, die eine AWS Config Regel verwenden, müssen Sie diese Ressourcen in aufzeichnen AWS Config. In dieser Tabelle ist auch angegeben, für welche Kontrollen eine bestimmte Ressource erforderlich ist. Ein Steuerelement benötigt möglicherweise mehr als eine Ressource.

Service	Erforderliche Ressource	Verwandte Kontrollen
Amazon API Gateway	`AWS::ApiGateway::Stage`	APIGateway.1 APIGateway.2 APIGateway.3 APIGateway.4 APIGateway.5
	`AWS::ApiGatewayV2::Stage`	APIGateway.1 APIGateway.9
AWS AppSync	`AWS::AppSync::GraphQLApi`	AppSync2.2 AppSync.4

Service	Erforderliche Ressource	Verwandte Kontrollen
		AppSync.5
AWS Backup (AWS Backup)	`AWS::Backup::RecoveryPoint`	Sicherung.1
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`	ACM.1 ACM.2 ACM. 3
Amazon Athena	`AWS::Athena::DataCatalog`	Athena.2
	`AWS::Athena::WorkGroup`	`Athena.3`
AWS CloudFormation	`AWS::CloudFormation::Stack`	CloudFormation1. CloudFormation.2

Service	Erforderliche Ressource	Verwandte Kontrollen
Amazon CloudFront	`AWS::CloudFront::Distribution`	CloudFront1. CloudFront.3 CloudFront.4 CloudFront.5 CloudFront.6 CloudFront.7 CloudFront.8 CloudFront.9 CloudFront.10 CloudFront.13 CloudFront.14
AWS CloudTrail	`AWS::CloudTrail::Trail`	CloudTrail.9
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	CloudWatch.15 CloudWatch.17
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	CodeArtifact1.

Service	Erforderliche Ressource	Verwandte Kontrollen
AWS CodeBuild	`AWS::CodeBuild::Project`	CodeBuild.1 CodeBuild.2 CodeBuild.3 CodeBuild.4
Amazon Detective	`AWS::Detective::Graph`	Detektiv.1
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate`	DMS.2

	`AWS::DMS::Endpoint`	`DMS.9`
		`DMS.10`
		`DMS.11`
		`DMS.12`

	`AWS::DMS::EventSubscription`	DMS.3
	`AWS::DMS::ReplicationInstance`	DMS.4 DMS.6
	`AWS::DMS::ReplicationSubnetGroup`	DMS. 5
	`AWS::DMS::ReplicationTask`	DMS. 7 DMS. 8

Service	Erforderliche Ressource	Verwandte Kontrollen
Amazon-DynamoDB	`AWS::DynamoDB::Table`	DynamoDB.2 Dynamo DB,6
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`	EC 2,51
	`AWS::EC2::CustomerGateway`	EC2,36
	`AWS::EC2::EIP`	EC2.12 EC2,37
	`AWS::EC2::FlowLog`	EC2,48
	`AWS::EC2::Instance`	EC2.4 EC2.8 EC2.9 EC2.17 EC2.24 EC2,38 EMR.1 SSM.1
	`AWS::EC2::InternetGateway`	EC2,39

Service	Erforderliche Ressource	Verwandte Kontrollen
	`AWS::EC2::LaunchTemplate`	EC2.25
	`AWS::EC2::NatGateway`	EC2,40
	`AWS::EC2::NetworkAcl`	EC2.16 EC2.21 EC2,41
	`AWS::EC2::NetworkInterface`	EC2.22 EC2,35
	`AWS::EC2::RouteTable`	EC2,42
	`AWS::EC2::SecurityGroup`	EC2.2 EC2.13 EC2,14 EC2.18 EC2.19 EC2,43

Service	Erforderliche Ressource	Verwandte Kontrollen
	`AWS::EC2::Subnet`	EC2.15 EC2,44 ElastiCache7. Lambda.5
	`AWS::EC2::TransitGateway`	EC2.23 EC2,52
	`AWS::EC2::TransitGatewayAttachment`	EC2,33
	`AWS::EC2::TransitGatewayRouteTable`	EC2,34
	`AWS::EC2::Volume`	EC2.3 EC2,45
	`AWS::EC2::VPC`	EC2,46
	`AWS::EC2::VPCEndpointService`	EC2,47
	`AWS::EC2::VPCPeeringConnector`	EC2,49

Service	Erforderliche Ressource	Verwandte Kontrollen
	`AWS::EC2::VPNConnection`	EC2.20
	`AWS::EC2::VPNGateway`	EC2,50
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	AutoScaling1. AutoScaling.2 AutoScaling.6 AutoScaling.9 AutoScaling.10
	`AWS::AutoScaling::LaunchConfiguration`	AutoScaling3. AutoScaling.5
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`	SSM.3
	`AWS::SSM::ManagedInstanceInventory`	SSM.1
	`AWS::SSM::PatchCompliance`	SSM.2

Service	Erforderliche Ressource	Verwandte Kontrollen
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`	ECR.4
	`AWS::ECR::Repository`	ECR.2 ECR.3
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`	ECS.12 SEK. 14
	`AWS::ECS::Service`	ECS.2 ECS.10 SEK. 13
	`AWS::ECS::TaskDefinition`	ECS.1 ECS.3 ECS.4 ECS.5 ECS.8 SEK. 9 SEK. 15
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`	EFS.3 EFS.4 EFS. 5

Service	Erforderliche Ressource	Verwandte Kontrollen
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`	EKS.2 EKS.6
	`AWS::EKS::IdentityProviderConfig`	EKS.7
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`	ElasticBeanstalk1. ElasticBeanstalk.2 ElasticBeanstalk.3
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`	ELB.2 ELB.3 ELB.5 ELB.7 ELB.8 ELB.9 ELB.10 ELB.14

Service	Erforderliche Ressource	Verwandte Kontrollen
	`AWS::ElasticLoadBalancingV2::LoadBalancer`	ELB.4 ELB.5 ELB.6 ELB.12 ELB.13 ELB. 16
ElasticSearch	`AWS::Elasticsearch::Domain`	ES.3 ES.4 ES.5 ES.6 ES.7 ES.8 ES.9
Amazon EventBridge	`AWS::Events::EventBus`	EventBridge2. EventBridge.3
	`AWS::Events::Endpoint`	EventBridge.4
`Amazon FSx`	`AWS::FSx::FileSystem`	FSX. 1

Service	Erforderliche Ressource	Verwandte Kontrollen
AWS Global Accelerator	AWS::GlobalAccelerator::Accelerator	GlobalAccelerator1.
AWS Glue	AWS::Glue::Job	Kleber.1
Amazon GuardDuty	AWS::GuardDuty::Detector	GuardDuty.4
	AWS::GuardDuty::Filter	GuardDuty.2
	AWS::GuardDuty::IPSet	GuardDuty.3
AWS Identity and Access Management (ICH BIN)	AWS::IAM::Group	IAM.18 ICH BIN 0,27 KMS.2
	AWS::IAM::Policy	IAM.1 IAM.21 KMS.1
	AWS::IAM::Role	IAM.18 ICH BIN 24 ICH BIN 27 KMS.2

Service	Erforderliche Ressource	Verwandte Kontrollen
	`AWS::IAM::User`	IAM.2 IAM.18 ICH BIN 25 ICH BIN 27 KMS.2
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	ICH BIN 23
AWS IoT	`AWS::IoT::Authorizer`	IoT.4
	`AWS::IoT::Dimension`	IoT.3
	`AWS::IoT::MitigationAction`	IoT.2
	`AWS::IoT::Policy`	IoT. 6
	`AWS::IoT::RoleAlias`	IoT.5
	`AWS::IoT::SecurityProfile`	IoT.1
AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`	KMS.3

Service	Erforderliche Ressource	Verwandte Kontrollen
Amazon Kinesis	`AWS::Kinesis::Stream`	Kinesis.1 Kinese.2
AWS Lambda	`AWS::Lambda::Function`	Lambda.1 Lambda.2 Lambda.3 Lambda.5 Lambda.6
Amazon MSK	`AWS::MSK::Cluster`	MASKE. 1 MSK.2
Amazon MQ	`AWS::AmazonMQ::Broker`	MQ. 2 MQ. 3 MQ. 4 MQ.5 MQ.6
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	NetworkFirewall1. NetworkFirewall.7 NetworkFirewall.9

Service	Erforderliche Ressource	Verwandte Kontrollen
	`AWS::NetworkFirewall::FirewallPolicy`	NetworkFirewall3. NetworkFirewall.4 NetworkFirewall.5 NetworkFirewall.8
	`AWS::NetworkFirewall::RuleGroup`	NetworkFirewall.6
OpenSearch Amazon-Dienst	`AWS::OpenSearch::Domain`	OpenSearch.1 OpenSearch.2 OpenSearch.3 OpenSearch.4 OpenSearch.5 OpenSearch.6 OpenSearch.7 OpenSearch.8 Suche öffnen.9 Öffne Suche.10 Öffne Suche.11

Service	Erforderliche Ressource	Verwandte Kontrollen
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`	DocumentDB DB.1 DocumentDB DB.2 DocumentDB DB.4 DocumentDB DB.5 Neptun.1 Neptun.2 Neptun.4 Neptun.5 Neptun.7 Neptun.8 Neptun.9 RDS.7 RDS.12 RDS.14 RDS.15 RDS.16 RDS.24 RDS. 27 RDS. 28 RDS. 34

Service	Erforderliche Ressource	Verwandte Kontrollen
		RDS.35
	`AWS::RDS::DBClusterSnapshot`	DocumentDB DB.3 Neptun.3 Neptun.6 RDS.1 RDS.4 RDS. 29

Service	Erforderliche Ressource	Verwandte Kontrollen
	`AWS::RDS::DBInstance`	RDS.2 RDS.3 RDS.5 RDS.6 RDS.8 RDS.9 RDS.10 RDS.11 RDS.13 RDS.17 RDS.18 RDS.23 RDS.25 RDS.30
	`AWS::RDS::DBSecurityGroup`	RDS. 31
	`AWS::RDS::DBSnapshot`	DocumentDB DB.3 RDS.1 RDS.4 RDS.32

Service	Erforderliche Ressource	Verwandte Kontrollen
	`AWS::RDS::DBSubnetGroup`	RDS.33
	`AWS::RDS::EventSubscription`	RDS.19 RDS.20 RDS.21 RDS.22
Amazon-Redshift	`AWS::Redshift::Cluster`	Redshift.1 Redshift.2 Redshift.3 Redshift.4 Redshift.6 Redshift.7 Redshift.8 Redshift.9 Redshift.10 Rotverschiebung.11
	`AWS::Redshift::ClusterParameterGroup`	Redshift.2

Service	Erforderliche Ressource	Verwandte Kontrollen
	`AWS::Redshift::ClusterSnapshot`	Rotverschiebung.13
	`AWS::Redshift::ClusterSubnetGroup`	Rotverschiebung.14
	`AWS::Redshift::EventSubscription`	Rotverschiebung.12
Amazon Route 53	`AWS::Route53::HostedZone`	Linie 53.2
Amazon-Simple-Storage-Service (Amazon-S3)	`AWS::S3::AccessPoint`	S3.19

Service	Erforderliche Ressource	Verwandte Kontrollen
	`AWS::S3::Bucket`	S3.2 S3.3 S3.5 S3.6 S3,7 S3.8 S3.9 S3.10 S3.11 S3.12 S3.13 S3.14 S3,15 S3,17 S3,20
AWS Secrets Manager	`AWS::SecretsManager::Secret`	SecretsManager1. SecretsManager.2 SecretsManager5.
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`	ServiceCatalog1.

Service	Erforderliche Ressource	Verwandte Kontrollen
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet`	SEE.2
	`AWS::SES::ContactList`	SESS.1
Amazon-Simple-Notification-Service (Amazon-SNS)	`AWS::SNS::Topic`	SNS.1 SNS.3
Amazon-Simple-Queue-Service (Amazon SQS)	`AWS::SQS::Queue`	SQS.1 SQS.2
Amazon SageMaker	`AWS::SageMaker::NotebookInstance`	SageMaker2. SageMaker.3
AWS Step Functions	`AWS::StepFunctions::StateMachine`	StepFunctions1. StepFunctions.2
AWS Transfer Family	`AWS::Transfer::Workflow`	Übertragung.1
AWS WAF	`AWS::WAF::Rule`	WAF.6
	`AWS::WAF::RuleGroup`	WAF.7
	`AWS::WAF::WebACL`	WAF.8
	`AWS::WAFRegional::Rule`	WAF.2

Service	Erforderliche Ressource	Verwandte Kontrollen
	`AWS::WAFRegional::RuleGroup`	WAF.3
	`AWS::WAFRegional::WebACL`	WAF.4
	`AWS::WAFv2::RuleGroup`	WAF.12
	`AWS::WAFv2::WebACL`	WAF.10

Erforderliche Ressourcen für den FSBP-Standard

Damit Security Hub die Ergebnisse für aktivierte, durch Änderungen ausgelöste Kontrollen von AWS Foundational Security Best Practices (FSBP), die eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie diese Ressourcen in aufzeichnen. AWS Config Weitere Informationen zu diesem Standard finden Sie unter. AWS FSBP-Standard (Basic Security Best Practices)

Service	Erforderliche -Ressourcen
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`

Service	Erforderliche -Ressourcen
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CodeBuild	`AWS::CodeBuild::Project`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint`
	`AWS::DMS::ReplicationInstance`
	`AWS::DMS::ReplicationTask`

Amazon-DynamoDB	`AWS::DynamoDB::Table`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`
	`AWS::EC2::Instance`
	`AWS::EC2::LaunchTemplate`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::TransitGateway`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Service	Erforderliche -Ressourcen
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon FSx	`AWS::FSx::FileSystem`

AWS Identity and Access Management (ICH BIN)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

Service	Erforderliche -Ressourcen
AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MSK	`AWS::MSK::Cluster`

AWS Network Firewall	`AWS::NetworkFirewall::Firewall`
	`AWS::NetworkFirewall::FirewallPolicy`
	`AWS::NetworkFirewall::RuleGroup`

OpenSearch Amazon-Dienst	`AWS::OpenSearch::Domain`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon-Redshift	`AWS::Redshift::Cluster`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon-Simple-Storage-Service (Amazon-S3)	`AWS::S3::AccessPoint` `AWS::S3::Bucket`
Amazon-Simple-Notification-Service (Amazon-SNS)	`AWS::SNS::Topic`
Amazon-Simple-Queue-Service (Amazon SQS)	`AWS::SQS::Queue`

Service	Erforderliche -Ressourcen
Amazon SageMaker	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Step Functions	`AWS::StepFunctions::StateMachine`

AWS WAF	`AWS::WAF::Rule`
	`AWS::WAF::RuleGroup`
	`AWS::WAF::WebACL`
	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::RuleGroup`
	`AWS::WAFv2::WebACL`

Erforderliche Ressourcen für CIS AWS Foundations Benchmark

Um Sicherheitsüberprüfungen für aktivierte Kontrollen durchzuführen, die für den Benchmark der Center for Internet Security (CIS) AWS Foundations gelten, führt Security Hub entweder genau die Prüfschritte durch, die für die Prüfungen in Securing Amazon Web Services vorgeschrieben sind, oder verwendet spezifische AWS Config verwaltete Regeln.

Weitere Informationen zu diesem Standard finden Sie unterCIS AWS Foundations Benchmark.

Erforderliche Ressourcen für CIS v3.0.0

Damit Security Hub die Ergebnisse für aktivierte, durch Änderungen ausgelöste CIS v3.0.0-Steuerelemente, die eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie diese Ressourcen in aufzeichnen. AWS Config

Service	Erforderliche -Ressourcen

Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::Instance`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::SecurityGroup`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::User`
	`AWS::IAM::Role`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon-Simple-Storage-Service (Amazon-S3)	`AWS::S3::Bucket`

Erforderliche Ressourcen für CIS v1.4.0

Damit Security Hub die Ergebnisse für aktivierte, durch Änderungen ausgelöste CIS v1.4.0-Steuerelemente, die eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie diese Ressourcen in AWS Config aufzeichnen.

Service	Erforderliche -Ressourcen
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::NetworkAcl` `AWS::EC2::SecurityGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` `AWS::IAM::User`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon-Simple-Storage-Service (Amazon-S3)	`AWS::S3::Bucket`

Erforderliche Ressourcen für CIS v1.2.0

Damit Security Hub die Ergebnisse für aktivierte, durch Änderungen ausgelöste CIS v1.2.0-Steuerelemente, die eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie diese Ressourcen in AWS Config aufzeichnen.

Service	Erforderliche -Ressourcen
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::SecurityGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` `AWS::IAM::User`

Erforderliche Ressourcen für NIST SP 800-53 Rev. 5

Damit Security Hub die Ergebnisse für aktivierte, durch Änderungen ausgelöste Kontrollen SP 800-53 Rev. 5 des National Institute of Standards and Technology (NIST), die eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie diese Ressourcen in aufzeichnen. AWS ConfigSie müssen nur Ressourcen für Kontrollen aufzeichnen, bei denen eine Änderung nach einem Zeitplan ausgelöst wurde. Weitere Informationen zu diesem Standard finden Sie unterNationales Institut für Standards und Technologie (NIST) SP 800-53 Rev. 5.

Service	Erforderliche -Ressourcen
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`

Service	Erforderliche -Ressourcen
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint`
	`AWS::DMS::ReplicationInstance`
	`AWS::DMS::ReplicationTask`

Amazon-DynamoDB	`AWS::DynamoDB::Table`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`
	`AWS::EC2::EIP`
	`AWS::EC2::Instance`
	`AWS::EC2::LaunchTemplate`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::TransitGateway`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`

Service	Erforderliche -Ressourcen
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::Endpoint` `AWS::Events::EventBus`
Amazon FSx	`AWS::FSx::FileSystem`

AWS Identity and Access Management (ICH BIN)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`

Service	Erforderliche -Ressourcen
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MSK	`AWS::MSK::Cluster`
Amazon MQ	`AWS::AmazonMQ::Broker`

AWS Network Firewall	`AWS::NetworkFirewall::Firewall`
	`AWS::NetworkFirewall::FirewallPolicy`
	`AWS::NetworkFirewall::RuleGroup`

OpenSearch Amazon-Dienst	`AWS::OpenSearch::Domain`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon-Redshift	`AWS::Redshift::Cluster`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon-Simple-Storage-Service (Amazon-S3)	`AWS::S3::AccessPoint` `AWS::S3::Bucket`
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
Amazon-Simple-Notification-Service (Amazon-SNS)	`AWS::SNS::Topic`

Service	Erforderliche -Ressourcen
Amazon-Simple-Queue-Service (Amazon SQS)	`AWS::SQS::Queue`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

Amazon SageMaker	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`

AWS WAF	`AWS::WAF::Rule`
	`AWS::WAF::RuleGroup`
	`AWS::WAF::WebACL`
	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::RuleGroup`
	`AWS::WAFv2::WebACL`

Erforderliche Ressourcen für PCI DSS v3.2.1

Damit Security Hub die Ergebnisse für aktivierte Kontrollen des Payment Card Industry Data Security Standard (PCI DSS), die eine AWS Config Regel verwenden, korrekt melden kann, müssen Sie diese Ressourcen in AWS Config aufzeichnen. Weitere Informationen zu diesem Standard finden Sie unterPayment Card Industry Data Security Standard (PCI DSS).

Service	Erforderliche -Ressourcen
AWS CodeBuild	`AWS::CodeBuild::Project`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::EIP`
	`AWS::EC2::Instance`
	`AWS::EC2::SecurityGroup`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
AWS Identity and Access Management (ICH BIN)	`AWS::IAM::Policy` `AWS::IAM::User`
AWS Lambda	`AWS::Lambda::Function`
OpenSearch Amazon-Dienst	`AWS::OpenSearch::Domain`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`

Amazon-Redshift	`AWS::Redshift::Cluster`
Amazon-Simple-Storage-Service (Amazon-S3)	`AWS::S3::Bucket`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

Erforderliche Ressourcen für AWS Resource Tagging Standard

Alle Steuerelemente im AWS Resource Tagging Standard werden durch Änderungen ausgelöst und verwenden eine AWS Config Regel. Damit Security Hub die Ergebnisse dieser Kontrollen korrekt melden kann, müssen Sie die folgenden Ressourcen in aufzeichnen AWS Config. Sie müssen nur Ressourcen für Kontrollen aufzeichnen, bei denen eine Änderung vom Typ eines Zeitplans ausgelöst wurde. Weitere Informationen zu diesem Standard finden Sie unterAWS Standard für die Kennzeichnung von Ressourcen.

Service	Erforderliche -Ressourcen
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS AppSync	`AWS::AppSync::GraphQLApi`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
Amazon Athena	`AWS::Athena::DataCatalog` `AWS::Athena::WorkGroup`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CloudTrail	`AWS::CloudTrail::Trail`
AWS CodeArtifact	`AWS::CodeArtifact::Repository`
Amazon Detective	`AWS::Detective::Graph`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate`
	`AWS::DMS::EventSubscription`
	`AWS::DMS::ReplicationInstance`

Service	Erforderliche -Ressourcen
	`AWS::DMS::ReplicationSubnetGroup`
Amazon-DynamoDB	`AWS::DynamoDB::Trail`

Service	Erforderliche -Ressourcen

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::CustomerGateway`
	`AWS::EC2::EIP`
	`AWS::EC2::FlowLog`
	`AWS::EC2::Instance`
	`AWS::EC2::InternetGateway`
	`AWS::EC2::NatGateway`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::RouteTable`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::TransitGateway`
	`AWS::EC2::TransitGatewayAttachment`
	`AWS::EC2::TransitGatewayRouteTable`
	`AWS::EC2::Volume`
	`AWS::EC2::VPC`
	`AWS::EC2::VPCEndpointService`
	`AWS::EC2::VPCPeeringConnector`
	`AWS::EC2::VPNGateway`

Service	Erforderliche -Ressourcen
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster` `AWS::EKS::IdentityProviderConfig`
AWS Elastic Beanstalk (Elastic Beanstalk)	`AWS::ElasticBeanstalk::Environment`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::EventBus`
AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`
AWS Glue	`AWS::Glue::Job`

Amazon GuardDuty	`AWS::GuardDuty::Detector`
	`AWS::GuardDuty::Filter`
	`AWS::GuardDuty::IPSet`

AWS Identity and Access Management (ICH BIN)	`AWS::IAM::Role` `AWS::IAM::User`
AWS Identity and Access Management Access Analyzer (IAM-Zugriffsanalysator)	`AWS::AccessAnalyzer::Analyzer`

Service	Erforderliche -Ressourcen

AWS IoT	`AWS::IoT::Authorizer`
	`AWS::IoT::Dimension`
	`AWS::IoT::MitigationAction`
	`AWS::IoT::Policy`
	`AWS::IoT::RoleAlias`
	`AWS::IoT::SecurityProfile`

Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` `AWS::NetworkFirewall::Firew allPolicy`
OpenSearch Amazon-Dienst	`AWS::OpenSearch::Domain`

Amazon Relational Database Service	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSecurityGroup`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::DBSubnetGroup`

Service	Erforderliche -Ressourcen

Amazon-Redshift	`AWS::Redshift::Cluster`
	`AWS::Redshift::ClusterSnapshot`
	`AWS::Redshift::ClusterSubnetGroup`
	`AWS::Redshift::EventSubscription`

AWS Secrets Manager	`AWS::SecretsManager::Secret`
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet` `AWS::SES::ContactList`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon-Simple-Queue-Service (Amazon SQS)	`AWS::SQS::Queue`
AWS Step Functions	`AWS::StepFunctions::Activity`
AWS Transfer Family	`AWS::Transfer::Workflow`

Erforderliche Ressourcen für Service-Managed Standard: AWS Control Tower

Damit Security Hub die Ergebnisse für aktivierte Service-Managed Standard: AWS Control Tower Change Triggered Controls, die eine AWS Config Regel verwenden, korrekt meldet, müssen Sie die folgenden Ressourcen in AWS Config aufzeichnen. Weitere Informationen zu diesem Standard finden Sie unterVom Service verwalteter Standard: AWS Control Tower.

Service	Erforderliche -Ressourcen
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`

Service	Erforderliche -Ressourcen
AWS CodeBuild	`AWS::CodeBuild::Project`
Amazon-DynamoDB	`AWS::DynamoDB::Table`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::Instance`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`

Service	Erforderliche -Ressourcen
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`

AWS Identity and Access Management (ICH BIN)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` `AWS::NetworkFirewall::RuleGroup`
OpenSearch Amazon-Dienst	`AWS::OpenSearch::Domain`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon-Redshift	`AWS::Redshift::Cluster`

Service	Erforderliche -Ressourcen
Amazon-Simple-Storage-Service (Amazon-S3)	`AWS::S3::Bucket`
Amazon-Simple-Notification-Service (Amazon-SNS)	`AWS::SNS::Topic`
Amazon-Simple-Queue-Service (Amazon SQS)	`AWS::SQS::Queue`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

AWS Secrets Manager	`AWS::SecretsManager::Secret`

AWS WAF	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::WebACL`

Zeitplan für die Ausführung von Sicherheitsprüfungen

Sobald Sie einen Sicherheitsstandard aktiviert haben AWS Security Hub , werden alle Prüfungen innerhalb von zwei Stunden ausgeführt. Die meisten Prüfungen werden innerhalb von 25 Minuten ausgeführt. Security Hub führt Prüfungen durch, indem es die Regel auswertet, die einer Kontrolle zugrunde liegt. Bis ein Steuerelement seinen ersten Prüflauf abgeschlossen hat, lautet sein Status Keine Daten.

Wenn Sie einen neuen Standard aktivieren, kann es bis zu 24 Stunden dauern, bis Security Hub Ergebnisse für Kontrollen generiert, die dieselbe zugrunde liegende AWS Config serviceverknüpfte Regel verwenden wie aktivierte Steuerelemente aus anderen aktivierten Standards. Wenn Sie beispielsweise Lambda.1 im Standard AWS Foundational Security Best Practices (FSBP) aktivieren, erstellt Security Hub die serviceverknüpfte Regel und generiert Ergebnisse in der Regel innerhalb von

Minuten. Wenn Sie danach Lambda.1 im Payment Card Industry Data Security Standard (PCI DSS) aktivieren, kann es bis zu 24 Stunden dauern, bis Security Hub Ergebnisse für dieses Steuerelement generiert, da es dieselbe serviceverknüpfte Regel wie Lambda.1 verwendet.

Nach der ersten Überprüfung kann der Zeitplan für jede Kontrolle entweder periodisch oder durch Änderung ausgelöst werden.

- Regelmäßige Prüfungen — Diese Prüfungen werden automatisch innerhalb von 12 oder 24 Stunden nach der letzten Ausführung ausgeführt. Security Hub bestimmt die Periodizität, und Sie können sie nicht ändern. Bei regelmäßigen Kontrollen erfolgt die Bewertung zu dem Zeitpunkt, zu dem die Prüfung ausgeführt wird. Wenn Sie den Workflow-Status eines periodischen Kontrollbefundes aktualisieren und dann bei der nächsten Überprüfung der Konformitätsstatus des Ergebnisses unverändert bleibt, bleibt der Workflow-Status in seinem geänderten Status. Wenn Sie beispielsweise eine fehlgeschlagene Suche für KMS.4 haben — die AWS KMS key Rotation sollte aktiviert sein und das Ergebnis anschließend korrigieren, ändert Security Hub den Workflow-Status von zu. `NEW` `RESOLVED` Wenn Sie die KMS-Schlüsselrotation vor der nächsten regelmäßigen Überprüfung deaktivieren, bleibt der Workflow-Status des Ergebnisses erhalten. `RESOLVED`
- Durch Änderungen ausgelöste Prüfungen — Diese Prüfungen werden ausgeführt, wenn sich der Status der zugehörigen Ressource ändert. AWS Config ermöglicht es Ihnen, zwischen der kontinuierlichen Aufzeichnung von Änderungen des Ressourcenstatus und der täglichen Aufzeichnung zu wählen. Wenn Sie die tägliche Aufzeichnung wählen AWS Config , werden die Ressourcenkonfigurationsdaten am Ende jedes 24-Stunden-Zeitraums bereitgestellt, wenn sich der Ressourcenstatus ändert. Wenn es keine Änderungen gibt, werden keine Daten geliefert. Dies kann die Generierung von Security Hub Hub-Ergebnissen verzögern, bis ein Zeitraum von 24 Stunden abgeschlossen ist. Unabhängig von Ihrem gewählten Aufnahmezeitraum überprüft Security Hub alle 18 Stunden, ob keine Ressourcen-Updates von verpasst AWS Config wurden.

Im Allgemeinen verwendet Security Hub nach Möglichkeit durch Änderungen ausgelöste Regeln. Damit eine Ressource eine durch Änderungen ausgelöste Regel verwenden kann, muss sie AWS Config Konfigurationselemente unterstützen.

Für ein Steuerelement, das auf einer verwalteten AWS Config Regel basiert, enthält die Beschreibung des Steuerelements einen Link zur Regelbeschreibung im AWS Config Entwicklerhandbuch. Zu dieser Beschreibung gehört auch, ob es sich bei der Regel um eine durch Änderung ausgelöste oder periodische Regel handelt.

Prüfungen, die benutzerdefinierte Lambda-Funktionen von Security Hub verwenden, werden regelmäßig durchgeführt.

Generierung und Aktualisierung der Kontrollergebnisse

AWS Security Hub generiert Ergebnisse, indem Prüfungen anhand von Sicherheitskontrollen durchgeführt werden. Für diese Ergebnisse wird das AWS Security Finding Format (ASFF) verwendet. Beachten Sie, dass das `Resource.Details` Objekt entfernt wird, wenn die Ergebnisgröße den Höchstwert von 240 KB überschreitet. Bei Steuerelementen, die durch AWS Config Ressourcen unterstützt werden, können Sie die Ressourcendetails in der AWS Config Konsole einsehen.

Security Hub berechnet normalerweise für jede Sicherheitskontrolle eine Gebühr. Wenn jedoch mehrere Kontrollen dieselbe AWS Config Regel verwenden, berechnet Security Hub für jede Überprüfung anhand der AWS Config Regel nur einmal eine Gebühr. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, generiert Security Hub ein einziges Ergebnis für eine Sicherheitsüberprüfung, auch wenn die Kontrolle in mehreren aktivierten Standards enthalten ist.

Die AWS Config Regel `iam-password-policy` wird beispielsweise von mehreren Kontrollen im Benchmark-Standard der Center for Internet Security (CIS) AWS Foundations und im Standard Foundational Security Best Practices verwendet. Jedes Mal, wenn Security Hub eine Überprüfung anhand dieser AWS Config Regel durchführt, generiert es ein separates Ergebnis für jede zugehörige Kontrolle, berechnet jedoch nur einmal für die Prüfung eine Gebühr.

Konsolidierte Kontrollergebnisse

Wenn konsolidierte Kontrollbefunde in Ihrem Konto aktiviert sind, generiert Security Hub für jede Sicherheitsüberprüfung einer Kontrolle ein einzelnes neues Ergebnis oder ein Befundupdate, auch wenn eine Kontrolle für mehrere aktivierte Standards gilt. Eine Liste der Kontrollen und der Standards, für die sie gelten, finden Sie unterReferenz zu Security Hub-Steuerungen. Sie können konsolidierte Kontrollergebnisse ein- oder ausschalten. Wir empfehlen, es einzuschalten, um das Suchgeräusch zu reduzieren.

Wenn Sie Security Hub AWS-Konto vor dem 23. Februar 2023 für einen aktiviert haben, müssen Sie die konsolidierten Kontrollergebnisse aktivieren, indem Sie den Anweisungen weiter unten in diesem Abschnitt folgen. Wenn Sie Security Hub am oder nach dem 23. Februar 2023 aktivieren, werden die konsolidierten Kontrollergebnisse in Ihrem Konto automatisch aktiviert. Wenn Sie jedoch die Security Hub Hub-Integration mit Mitgliedskonten verwenden AWS Organizations oder Mitgliedskonten über einen manuellen Einladungsprozess eingeladen haben, wird die konsolidierte Kontrollermittlung in Mitgliedskonten nur aktiviert, wenn sie im Administratorkonto aktiviert ist. Wenn die Funktion im Administratorkonto deaktiviert ist, ist sie auch in den Mitgliedskonten deaktiviert. Dieses Verhalten gilt für neue und bestehende Mitgliedskonten.

Wenn Sie konsolidierte Kontrollergebnisse in Ihrem Konto deaktivieren, generiert Security Hub für jeden aktivierten Standard, der eine Kontrolle enthält, ein separates Ergebnis pro Sicherheitsprüfung. Wenn sich beispielsweise vier aktivierte Standards eine Kontrolle mit derselben zugrunde liegenden AWS Config Regel teilen, erhalten Sie nach einer Sicherheitsprüfung der Kontrolle vier separate Ergebnisse. Wenn Sie die Option „Ergebnisse konsolidierter Kontrollen“ aktivieren, erhalten Sie nur ein Ergebnis. Weitere Informationen darüber, wie sich die Konsolidierung auf Ihre Ergebnisse auswirkt, finden Sie unterErgebnisse der Stichprobenkontrolle.

Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erstellt Security Hub neue standardunabhängige Ergebnisse und archiviert die ursprünglichen standardbasierten Ergebnisse. Einige Felder und Werte für Kontrollergebnisse werden sich ändern und können sich auf bestehende Workflows auswirken. Weitere Informationen zu diesen Änderungen finden Sie unter Konsolidierte Kontrollergebnisse — ASFF-Änderungen.

Die Aktivierung konsolidierter Kontrollergebnisse kann sich auch auf die Ergebnisse auswirken, die Integrationen von Drittanbietern von Security Hub erhalten. Automated Security Response auf AWS Version 2.0.0 unterstützt konsolidierte Kontrollergebnisse.

Die konsolidierten Kontrollergebnisse werden aktiviert

Um konsolidierte Kontrollergebnisse zu aktivieren, müssen Sie mit einem Administratorkonto oder einem eigenständigen Konto angemeldet sein.

> **Note**
>
> Nach der Aktivierung der konsolidierten Kontrollergebnisse kann es bis zu 24 Stunden dauern, bis Security Hub neue, konsolidierte Ergebnisse generiert und die ursprünglichen, standardbasierten Ergebnisse archiviert hat. Während dieser Zeit kann es sein, dass Sie in Ihrem Konto eine Mischung aus standardunabhängigen und standardbasierten Ergebnissen sehen.

Security Hub console

1. Öffnen Sie die Konsole unter https://console.aws.amazon.com/securityhub/. AWS Security Hub
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie die Registerkarte Allgemein.

4. Aktivieren Sie für Kontrollen die Option Konsolidierte Kontrollergebnisse.
5. Wählen Sie Speichern.

Security Hub API

1. Führen Sie `UpdateSecurityHubConfiguration`.
2. Auf `ControlFindingGenerator` gleich setzen`SECURITY_CONTROL`.

   Beispiel für eine Anfrage:

```
{
   "ControlFindingGenerator": "SECURITY_CONTROL"
}
```

AWS CLI

1. Führen Sie den Befehl `update-security-hub-configuration` aus.
2. `control-finding-generator`Gleich setzen`SECURITY_CONTROL`.

```
aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

Deaktivierung konsolidierter Kontrollergebnisse

Um konsolidierte Kontrollbefunde zu deaktivieren, müssen Sie mit einem Administratorkonto oder einem eigenständigen Konto angemeldet sein.

> **Note**
>
> Nach dem Deaktivieren der konsolidierten Kontrollergebnisse kann es bis zu 24 Stunden dauern, bis Security Hub neue, standardbasierte Ergebnisse generiert und die konsolidierten Ergebnisse archiviert hat. Während dieser Zeit kann es sein, dass Sie in Ihrem Konto eine Mischung aus standardbasierten und konsolidierten Ergebnissen sehen.

Security Hub console

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie die Registerkarte Allgemein.
4. Wählen Sie für Kontrollen die Option Bearbeiten und deaktivieren Sie die Option Konsolidierte Kontrollergebnisse.
5. Wählen Sie Speichern.

Security Hub API

1. Führen Sie `UpdateSecurityHubConfiguration`.
2. Auf `ControlFindingGenerator` gleich setzen`STANDARD_CONTROL`.

   Beispiel für eine Anfrage:

```
{
   "ControlFindingGenerator": "STANDARD_CONTROL"
}
```

AWS CLI

1. Führen Sie den Befehl `update-security-hub-configuration` aus.
2. `control-finding-generator`Gleich setzen`STANDARD_CONTROL`.

```
aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

`Compliance`Einzelheiten zu den Kontrollbefunden

Bei Ergebnissen, die bei Sicherheitskontrollen festgestellt wurden, enthält das `Compliance`Feld im AWS Security Finding Format (ASFF) Einzelheiten zu den Kontrollfeststellungen. Das Feld `Compliance` enthält die folgenden Informationen.

`AssociatedStandards`

Die aktivierten Standards, nach denen ein Steuerelement aktiviert ist.

`RelatedRequirements`

Die Liste der zugehörigen Anforderungen für die Steuerung in allen aktivierten Standards. Die Anforderungen stammen aus dem Sicherheitsrahmen eines Drittanbieters für die Kontrolle, z. B. dem Payment Card Industry Data Security Standard (PCI DSS).

`SecurityControlId`

Die Kennung für eine Kontrolle aller Sicherheitsstandards, die Security Hub unterstützt.

`Status`

Das Ergebnis der letzten Überprüfung, die Security Hub für ein bestimmtes Steuerelement ausgeführt hat. Die Ergebnisse der vorherigen Überprüfungen werden 90 Tage lang archiviert.

`StatusReasons`

Enthält eine Liste von Gründen für den Wert von`Compliance.Status`. `StatusReasons` enthält für jeden Grund den Ursachencode und eine Beschreibung.

In der folgenden Tabelle sind die verfügbaren Status-Ursachencodes und Beschreibungen aufgeführt. Die Behebungsschritte hängen davon ab, welche Kontrolle einen Befund mit dem Ursachencode generiert hat. Wählen Sie ein Steuerelement ausReferenz zu Security Hub-Steuerungen, um die Behebungsschritte für dieses Steuerelement anzuzeigen.

Ursachencode	Compliance.Status	Beschreibung
`CLOUDTRAIL_METRIC_FILTER_NOT_VALID`	`FAILED`	Für den CloudTrail Trail mit mehreren Regionen gibt es keinen gültigen metrischen Filter.
`CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT`	`FAILED`	Metrische Filter sind für den Trail mit mehreren Regionen CloudTrail nicht vorhanden.

Ursachencode	Compliance.Status	Beschreibung
`CLOUDTRAIL_MULTI_REGION_NOT_PRESENT`	`FAILED`	Das Konto verfügt nicht über einen multiregionalen CloudTrail Trail mit der erforderlichen Konfiguration.
`CLOUDTRAIL_REGION_INVAILD`	`WARNING`	CloudTrail Wanderwege mit mehreren Regionen befinden sich nicht in der aktuellen Region.
`CLOUDWATCH_ALARM_ACTIONS_NOT_VALID`	`FAILED`	Es sind keine gültigen Alarmaktionen vorhanden.
`CLOUDWATCH_ALARMS_NOT_PRESENT`	`FAILED`	CloudWatch Alarme sind im Konto nicht vorhanden.
`CONFIG_ACCESS_DENIED`	`NOT_AVAILABLE` AWS Config Status ist `ConfigError`	AWS Config Zugriff verweigert. Stellen Sie sicher, dass es aktiviert AWS Config ist und dass ihm ausreichende Berechtigungen erteilt wurden.
`CONFIG_EVALUATIONS_EMPTY`	`PASSED`	AWS Config hat Ihre Ressourcen anhand der Regel bewertet. Die Regel galt nicht für die AWS Ressourcen in ihrem Geltungsbereich, die angegebenen Ressourcen wurden gelöscht oder die Bewertungsergebnisse wurden gelöscht.

Ursachencode	Compliance.Status	Beschreibung
`CONFIG_RETURNS_NOT_APPLICABLE`	`NOT_AVAILABLE`	Der Konformitätsstatus ist darauf `NOT_AVAILABLE` zurückzuführen, dass der Status Nicht zutreffend AWS Config zurückgegeben wurde. AWS Config gibt keinen Grund für den Status an. Hier sind einige mögliche Gründe für den Status „Nicht zutreffend“: • Die Ressource wurde aus dem Geltungsbereich der AWS Config Regel entfernt. • Die AWS Config Regel wurde gelöscht. • Die Ressource wurde gelöscht. • Die AWS Config Regellogik kann den Status Nicht zutreffend erzeugen.

Ursachencode	Compliance.Status	Beschreibung
`CONFIG_RULE_EVALUATION_ERROR`	`NOT_AVAILABLE` AWS Config Der Status ist `ConfigError`	Dieser Ursachencode wird für verschiedene Arten von Auswertungsfehlern verwendet. Die Beschreibung enthält die spezifischen Ursacheninformationen. Die Art des Fehlers kann einer der folgenden sein: • Unmöglichkeit, die Auswertung aufgrund fehlender Berechtigungen durchzuführen. Die Beschreibung enthält die spezifische Berechtigung, die fehlt. • Ein fehlender oder ungültiger Wert für einen Parameter. Die Beschreibung enthält den Parameter und die Anforderungen für den Parameterwert. • Fehler beim Lesen aus einem S3-Bucket. Die Beschreibung identifiziert den Bucket und stellt den spezifischen Fehler bereit. • Ein fehlendes AWS Abonnement. • Ein allgemeines Timeout für die Auswertung. • Ein gesperrtes Konto.

Ursachencode	Compliance.Status	Beschreibung
`CONFIG_RULE_NOT_FOUND`	`NOT_AVAILABLE` AWS Config Status ist `ConfigError`	Die AWS Config Regel wird gerade erstellt.
`INTERNAL_SERVICE_ERROR`	`NOT_AVAILABLE`	Es ist ein unbekannter Fehler aufgetreten.
`LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE`	FEHLGESCHLAGEN	Security Hub kann keine Überprüfung anhand einer benutzerdefinierten Lambda-Laufzeit durchführen.
`S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION`	`WARNING`	Das Ergebnis befindet sich in einem `WARNING` Status, da sich der S3-Bucket, der dieser Regel zugeordnet ist, in einer anderen Region oder einem anderen Konto befindet. Diese Regel unterstützt keine regionsübergreifenden oder kontenübergreifenden Prüfungen. Es wird empfohlen, diese Kontrolle in dieser Region oder diesem Konto zu deaktivieren. Führen Sie sie nur in der Region oder dem Konto aus, in dem sich die Ressource befindet.
`SNS_SUBSCRIPTION_NOT_PRESENT`	`FAILED`	Die CloudWatch Logs-Metrikfilter haben kein gültiges Amazon SNS SNS-Abonnement.

Ursachencode	Compliance.Status	Beschreibung
SNS_TOPIC_CROSS_ACCOUNT	WARNING	Das Ergebnis befindet sich in einem WARNING Zustand. Das mit dieser Regel verknüpfte SNS-Thema gehört einem anderen Konto. Das aktuelle Konto kann die Abonnementinformationen nicht abrufen. Das Konto, dem das SNS-Thema gehört, muss dem aktuellen Konto die sns:ListSubscriptionsByTopic Berechtigung für das SNS-Thema gewähren.
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	Das Ergebnis weist einen WARNING Status auf, da sich das mit dieser Regel verknüpfte SNS-Thema in einer anderen Region oder einem anderen Konto befindet. Diese Regel unterstützt keine regionsübergreifenden oder kontenübergreifenden Prüfungen. Es wird empfohlen, diese Kontrolle in dieser Region oder diesem Konto zu deaktivieren. Führen Sie sie nur in der Region oder dem Konto aus, in dem sich die Ressource befindet.
SNS_TOPIC_INVALID	FAILED	Das mit dieser Regel verknüpfte SNS-Thema ist ungültig.

Ursachencode	Compliance.Status	Beschreibung
THROTTLING_ERROR	NOT_AVAILABLE	Die entsprechende API-Operation hat die zulässige Rate überschritten.

ProductFieldsEinzelheiten zu den Kontrollbefunden

Wenn Security Hub Sicherheitsprüfungen durchführt und Kontrollergebnisse generiert, umfasst das `ProductFields` Attribut in ASFF die folgenden Felder:

`ArchivalReasons:0/Description`

Beschreibt, warum Security Hub bestehende Ergebnisse archiviert hat.

Security Hub archiviert beispielsweise vorhandene Ergebnisse, wenn Sie eine Kontrolle oder einen Standard deaktivieren und wenn Sie konsolidierte Kontrollergebnisse ein- oder ausschalten.

`ArchivalReasons:0/ReasonCode`

Gibt den Grund an, warum Security Hub bestehende Ergebnisse archiviert hat.

Security Hub archiviert beispielsweise vorhandene Ergebnisse, wenn Sie eine Kontrolle oder einen Standard deaktivieren und wenn Sie konsolidierte Kontrollergebnisse ein- oder ausschalten.

`StandardsGuideArn` oder `StandardsArn`

Der ARN des Standards, der dem Steuerelement zugeordnet ist.

Für den Benchmark-Standard der CIS AWS Foundations lautet das Feld`StandardsGuideArn`.

Für die Standards PCI DSS und AWS Foundational Security Best Practices lautet das Feld. `StandardsArn`

Diese Felder werden zugunsten von entfernt, `Compliance.AssociatedStandards` wenn Sie die Option „Konsolidierte Kontrollergebnisse“ aktivieren.

`StandardsGuideSubscriptionArn` oder `StandardsSubscriptionArn`

Der ARN des Standardabonnements des Kontos.

Für den Benchmark-Standard der CIS AWS Foundations lautet das Feld`StandardsGuideSubscriptionArn`.

Für die Standards PCI DSS und AWS Foundational Security Best Practices lautet das Feld. `StandardsSubscriptionArn`

Diese Felder werden entfernt, wenn Sie die Option „Konsolidierte Kontrollergebnisse“ aktivieren.

`RuleId` oder `ControlId`

Die Kennung der Kontrolle.

Für den Benchmark-Standard der CIS AWS Foundations lautet das Feld`RuleId`.

Für andere Standards ist das Feld`ControlId`.

Diese Felder werden zugunsten von entfernt, `Compliance.SecurityControlId` wenn Sie konsolidierte Kontrollergebnisse aktivieren.

`RecommendationUrl`

Die URL zu den Behebungsinformationen für die Kontrolle. Dieses Feld wird entfernt, `Remediation.Recommendation.Url` wenn Sie konsolidierte Kontrollergebnisse aktivieren.

`RelatedAWSResources:0/name`

Der Name der Ressource, die dem Ergebnis zugeordnet ist.

`RelatedAWSResource:0/type`

Der Typ der Ressource, die dem Steuerelement zugeordnet ist.

`StandardsControlArn`

Der ARN des Steuerelements. Dieses Feld wird entfernt, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

`aws/securityhub/ProductName`

Für Ergebnisse, die auf Kontrollen basieren, lautet der Produktname Security Hub.

`aws/securityhub/CompanyName`

Für Ergebnisse, die auf Kontrollen basieren, lautet der Firmenname. AWS

`aws/securityhub/annotation`

Eine Beschreibung des von der Kontrolle aufgedeckten Problems.

`aws/securityhub/FindingId`

Die Kennung des Befundes. Dieses Feld verweist nicht auf einen Standard, wenn Sie konsolidierte Kontrollergebnisse aktivieren.

Den Kontrollergebnissen den Schweregrad zuweisen

Der Schweregrad, der einem Security Hub-Steuerelement zugewiesen wurde, zeigt die Wichtigkeit der Kontrolle an. Der Schweregrad einer Kontrolle bestimmt den Schweregrad, der den Kontrollergebnissen zugewiesen wird.

Schweregradkriterien

Der Schweregrad einer Kontrolle wird anhand der folgenden Kriterien bestimmt:

- Wie schwierig ist es für einen Bedrohungsakteur, die mit der Kontrolle verbundene Konfigurationsschwäche auszunutzen?

  Die Schwierigkeit wird durch den Grad an Raffinesse oder Komplexität bestimmt, der erforderlich ist, um die Schwachstelle zur Ausführung eines Bedrohungsszenarios auszunutzen.
- Wie wahrscheinlich ist es, dass die Schwachstelle zu einer Beeinträchtigung Ihrer Ressourcen AWS-Konten oder Ihrer Ressourcen führt?

  Eine Beeinträchtigung Ihrer AWS-Konten Ressourcen bedeutet, dass die Vertraulichkeit, Integrität oder Verfügbarkeit Ihrer Daten oder AWS Infrastruktur in irgendeiner Weise beeinträchtigt wird.

  Die Wahrscheinlichkeit einer Gefährdung gibt an, wie wahrscheinlich es ist, dass das Bedrohungsszenario zu einer Unterbrechung oder Verletzung Ihrer AWS Dienste oder Ressourcen führt.

Betrachten Sie als Beispiel die folgenden Konfigurationsschwächen:

- Benutzerzugriffsschlüssel werden nicht alle 90 Tage ausgetauscht.
- Der IAM-Root-Benutzerschlüssel ist vorhanden.

Beide Schwächen sind für einen Gegner gleichermaßen schwer auszunutzen. In beiden Fällen kann der Angreifer Anmeldeinformationen stehlen oder eine andere Methode verwenden, um an einen Benutzerschlüssel zu gelangen. Er kann es dann verwenden, um auf unautorisierte Weise auf Ihre Ressourcen zuzugreifen.

Die Wahrscheinlichkeit einer Kompromittierung ist jedoch viel höher, wenn der Bedrohungsakteur den Root-Benutzerzugriffsschlüssel erwirbt, da er dadurch besseren Zugriff hat. Infolgedessen hat die Schwäche des Root-Benutzerschlüssels einen höheren Schweregrad.

Der Schweregrad berücksichtigt nicht die Wichtigkeit der zugrunde liegenden Ressource. Kritikalität ist der Grad der Wichtigkeit der Ressourcen, die mit dem Ergebnis verknüpft sind. Beispielsweise ist eine Ressource, die einer geschäftskritischen Anwendung zugeordnet ist, kritischer als eine, die nicht produktionstechnischen Tests zugeordnet ist. Verwenden Sie das `Criticality` Feld des AWS Security Finding Format (ASFF), um Informationen zur Ressourcenkritik zu erfassen.

In der folgenden Tabelle werden die Sicherheitslabel den Schwierigkeiten bei der Ausnutzung und der Wahrscheinlichkeit einer Gefährdung zugeordnet.

	Ein Kompromiss ist sehr wahrscheinlich	Kompromiss wahrscheinlich	Kompromiss unwahrscheinlich	Ein Kompromiss ist höchst unwahrscheinlich
Sehr einfach auszunutzen	Kritisch	Kritisch	Hoch	Mittelschwer
Etwas einfach auszunutzen	Kritisch	Hoch	Mittelschwer	Mittelschwer
Etwas schwer auszunutzen	Hoch	Mittelschwer	Mittelschwer	Niedrig
Sehr schwer auszunutzen	Mittelschwer	Mittelschwer	Niedrig	Niedrig

Definitionen des Schweregrads

Die Schweregrade sind wie folgt definiert.

Kritisch — Das Problem sollte sofort behoben werden, um eine Eskalation zu vermeiden.

> Beispielsweise wird ein offener S3-Bucket mit kritischem Schweregrad bewertet. Da so viele Bedrohungsakteure nach offenen S3-Buckets suchen, ist es wahrscheinlich, dass Daten in exponierten S3-Buckets von anderen entdeckt und abgerufen werden.
>
> Im Allgemeinen gelten öffentlich zugängliche Ressourcen als kritische Sicherheitslücken. Sie sollten kritische Ergebnisse mit äußerster Dringlichkeit behandeln. Sie sollten auch die Wichtigkeit der Ressource berücksichtigen.

Hoch — Das Problem muss als kurzfristige Priorität angegangen werden.

Wenn eine Standard-VPC-Sicherheitsgruppe beispielsweise für eingehenden und ausgehenden Datenverkehr geöffnet ist, wird sie als hochgradig eingestuft. Für einen Bedrohungsakteur ist es ziemlich einfach, eine VPC mit dieser Methode zu kompromittieren. Es ist auch wahrscheinlich, dass der Bedrohungsakteur in der Lage sein wird, Ressourcen zu unterbrechen oder zu exfiltrieren, sobald sie sich in der VPC befinden.

Security Hub empfiehlt, dass Sie einen Befund mit hohem Schweregrad als kurzfristige Priorität behandeln. Sie sollten sofort Abhilfemaßnahmen ergreifen. Sie sollten auch die Wichtigkeit der Ressource berücksichtigen.

Mittel — Das Problem sollte als mittelfristige Priorität behandelt werden.

Mangelnde Verschlüsselung für Daten bei der Übertragung wird beispielsweise als mittelgradig eingestuft. Um diese Schwachstelle auszunutzen, ist ein ausgeklügelter man-in-the-middle Angriff erforderlich. Mit anderen Worten, es ist etwas schwierig. Es ist wahrscheinlich, dass einige Daten gefährdet werden, wenn das Bedrohungsszenario erfolgreich ist.

Security Hub empfiehlt, dass Sie die betroffene Ressource so schnell wie möglich untersuchen. Sie sollten auch die Wichtigkeit der Ressource berücksichtigen.

Niedrig — Das Problem erfordert keine eigenständigen Maßnahmen.

Beispielsweise wird das Versäumnis, forensische Informationen zu sammeln, als niedriger Schweregrad angesehen. Diese Kontrolle kann dazu beitragen, future Kompromisse zu verhindern, aber das Fehlen von Forensik führt nicht direkt zu einem Kompromiss.

Bei Ergebnissen mit geringem Schweregrad müssen Sie nicht sofort Maßnahmen ergreifen, aber sie können einen Kontext bieten, wenn Sie sie mit anderen Problemen korrelieren.

Informativ — Es wurde keine Sicherheitslücke in der Konfiguration gefunden.

Mit anderen Worten, der Status ist `PASSEDWARNING`, oder`NOT AVAILABLE`.

Es gibt keine empfohlene Aktion. Informationsergebnisse helfen Kunden dabei, nachzuweisen, dass sie sich in einem konformen Zustand befinden.

Regeln für die Aktualisierung der Kontrollergebnisse

Eine nachfolgende Überprüfung anhand einer bestimmten Regel kann zu einem neuen Ergebnis führen. Beispielsweise könnte der Status „Verwendung des Root-Benutzers vermeiden“ von `FAILED`

zu geändert PASSED werden. In diesem Fall wird ein neues Ergebnis generiert, das das neueste Ergebnis enthält.

Wenn eine nachfolgende Überprüfung basierend auf einer bestimmten Regel ein Ergebnis generiert, das mit dem aktuellen Ergebnis übereinstimmt, wird das bestehende Ergebnis aktualisiert. Es wird kein neues Ergebnis generiert.

Security Hub archiviert automatisch Ergebnisse von Kontrollen, wenn die zugehörige Ressource gelöscht wird, die Ressource nicht existiert oder die Kontrolle deaktiviert ist. Eine Ressource ist möglicherweise nicht mehr vorhanden, da der zugehörige Dienst derzeit nicht verwendet wird. Die Ergebnisse werden automatisch auf der Grundlage eines der folgenden Kriterien archiviert:

- Die Ergebnisse werden drei bis fünf Tage lang nicht aktualisiert (beachten Sie, dass dies nach bestem Wissen erfolgt und nicht garantiert wird).
- Die zugehörige AWS Config Bewertung wurde zurückgegebenNOT_APPLICABLE.

Konformitätsstatus und Kontrollstatus

Das Compliance.Status Feld „Format für AWS Sicherheitsbefunde“ beschreibt das Ergebnis eines Kontrollergebnisses. Security Hub verwendet den Compliance-Status der Kontrollergebnisse, um einen allgemeinen Kontrollstatus zu ermitteln. Der Kontrollstatus wird auf der Detailseite einer Kontrolle in der Security Hub Hub-Konsole angezeigt.

Bei einem Administratorkonto spiegelt der Kontrollstatus den Kontrollstatus im Administratorkonto und in den Mitgliedskonten wider. Insbesondere wird der Gesamtstatus eines Steuerelements als Fehlgeschlagen angezeigt, wenn für das Steuerelement ein oder mehrere fehlerhafte Ergebnisse im Administratorkonto oder in einem der Mitgliedskonten gefunden wurden. Wenn Sie eine Aggregationsregion festgelegt haben, spiegelt der Kontrollstatus in der Aggregationsregion den Kontrollstatus in der Aggregationsregion und den verknüpften Regionen wider. Insbesondere wird der Gesamtstatus eines Steuerelements als Fehlgeschlagen angezeigt, wenn für das Steuerelement ein oder mehrere fehlgeschlagene Ergebnisse in der Aggregationsregion oder einer der verknüpften Regionen vorliegen.

Security Hub generiert den anfänglichen Kontrollstatus in der Regel innerhalb von 30 Minuten nach Ihrem ersten Besuch der Übersichtsseite oder der Seite Sicherheitsstandards der Security Hub Hub-Konsole. Sie müssen die AWS Config Ressourcenaufzeichnung konfiguriert haben, damit der Kontrollstatus angezeigt wird. Nachdem die Kontrollstatus zum ersten Mal generiert wurden, aktualisiert Security Hub die Kontrollstatus alle 24 Stunden auf der Grundlage der Ergebnisse

der letzten 24 Stunden. Ein Zeitstempel auf der Seite mit den Kontrolldetails gibt an, wann der Kontrollstatus zuletzt aktualisiert wurde.

> **Note**
>
> Nach der Aktivierung eines Steuerelements kann es bis zu 24 Stunden dauern, bis zum ersten Mal Kontrollstatus in den chinesischen Regionen und generiert werden. AWS GovCloud (US) Region

Werte für den Konformitätsstatus eines Ergebnisses

Dem Konformitätsstatus für jedes Ergebnis wird einer der folgenden Werte zugewiesen:

- `PASSED`— Zeigt an, dass das Steuerelement die Sicherheitsüberprüfung für dieses Ergebnis bestanden hat. Setzt den Security Hub automatisch `Workflow.Status` auf`RESOLVED`.

  Ändert sich `Compliance.Status` für ein Ergebnis von `PASSED` zu `FAILEDWARNING`, oder`NOT_AVAILABLE`, und `Workflow.Status` war entweder `NOTIFIED` oder`RESOLVED`, dann setzt Security Hub automatisch `Workflow.Status` auf`NEW`.

  Wenn Sie nicht über Ressourcen verfügen, die einer Kontrolle entsprechen, generiert Security Hub einen `PASSED` Befund auf Kontoebene. Wenn Sie eine Ressource haben, die einem Steuerelement entspricht, die Ressource dann aber löschen, erstellt Security Hub einen `NOT_AVAILABLE` Befund und archiviert ihn sofort. Nach 18 Stunden erhalten Sie einen `PASSED` Befund, da Sie nicht mehr über Ressourcen verfügen, die der Kontrolle entsprechen.
- `FAILED`— Zeigt an, dass die Kontrolle die Sicherheitsüberprüfung für diesen Befund nicht bestanden hat.
- `WARNING`— Zeigt an, dass die Prüfung abgeschlossen wurde, Security Hub jedoch nicht feststellen kann, ob sich die Ressource im `FAILED` Status `PASSED` oder befindet.
- `NOT_AVAILABLE`— Zeigt an, dass die Prüfung nicht abgeschlossen werden kann, weil ein Server ausgefallen ist, die Ressource gelöscht wurde `NOT_APPLICABLE` oder das Ergebnis der AWS Config Auswertung

  Wenn das AWS Config Evaluierungsergebnis war`NOT_APPLICABLE`, archiviert Security Hub den Befund automatisch.

Werte für den Kontrollstatus

Security Hub leitet aus dem Compliance-Status der Kontrollfeststellungen einen allgemeinen Kontrollstatus ab. Bei der Bestimmung des Kontrollstatus ignoriert Security Hub Ergebnisse mit einem `RecordState` von `ARCHIVED` und Ergebnisse mit einem `Workflow.Status` von`SUPPRESSED`.

Dem Kontrollstatus wird einer der folgenden Werte zugewiesen:

- Bestanden — Zeigt an, dass alle Ergebnisse den Konformitätsstatus haben`PASSED`.
- Fehlgeschlagen — Zeigt an, dass mindestens ein Ergebnis den Konformitätsstatus hat`FAILED`.
- Unbekannt — Gibt an, dass mindestens ein Ergebnis den Konformitätsstatus `WARNING` oder hat`NOT_AVAILABLE`. Keine Ergebnisse haben den Konformitätsstatus`FAILED`.
- Keine Daten — Zeigt an, dass keine Ergebnisse für die Kontrolle vorliegen. Beispielsweise hat ein neu aktiviertes Steuerelement diesen Status, bis Security Hub beginnt, Ergebnisse dafür zu generieren. Ein Steuerelement hat diesen Status auch, wenn alle Ergebnisse in der aktuellen Region nicht verfügbar sind `SUPPRESSED` oder nicht verfügbar sind.
- Deaktiviert — Zeigt an, dass das Steuerelement im aktuellen Konto und in der Region deaktiviert ist. Für dieses Steuerelement werden derzeit keine Sicherheitsüberprüfungen im Girokonto und in der Region durchgeführt. Die Ergebnisse einer deaktivierten Kontrolle können sich jedoch bis zu 24 Stunden nach der Deaktivierung auf den Compliance-Status auswirken.

Ermittlung von Sicherheitseinstufungen

Auf der Übersichtsseite und der Kontrollseite der Security Hub Hub-Konsole wird eine Zusammenfassung der Sicherheitsbewertung für alle Ihre aktivierten Standards angezeigt. Auf der Seite Sicherheitsstandards zeigt Security Hub außerdem eine Sicherheitsbewertung von 0 bis 100 Prozent für jeden aktivierten Standard an.

Wenn Sie Security Hub zum ersten Mal aktivieren, berechnet Security Hub die zusammenfassende Sicherheitsbewertung und die Standardsicherheitsbewertungen innerhalb von 30 Minuten nach Ihrem ersten Besuch der Übersichtsseite oder der Seite Sicherheitsstandards in der Security Hub Hub-Konsole. Bewertungen werden nur für Standards generiert, die aktiviert sind, wenn Sie diese Seiten besuchen. Rufen Sie den `GetEnabledStandards`API-Vorgang auf, um eine Liste der derzeit aktivierten Standards anzuzeigen. Darüber hinaus muss die AWS Config Ressourcenaufzeichnung konfiguriert werden, damit die Ergebnisse angezeigt werden. Die zusammenfassende Sicherheitsbewertung ist der Durchschnitt der Standardsicherheitsbewertungen.

Nach der erstmaligen Generierung der Ergebnisse aktualisiert Security Hub die Sicherheitswerte alle 24 Stunden. Security Hub zeigt einen Zeitstempel an, der angibt, wann eine Sicherheitsbewertung zuletzt aktualisiert wurde.

> **Note**
>
> In den chinesischen Regionen und kann es bis zu 24 Stunden dauern, bis zum ersten Mal Sicherheitsbewertungen generiert werden. AWS GovCloud (US) Region

Wenn Sie die Option „Konsolidierte Kontrollergebnisse“ aktivieren, kann es bis zu 24 Stunden dauern, bis Ihre Sicherheitsbewertungen aktualisiert werden. Darüber hinaus werden durch die Aktivierung einer neuen Aggregationsregion oder die Aktualisierung verknüpfter Regionen bestehende Sicherheitsbewertungen zurückgesetzt. Es kann bis zu 24 Stunden dauern, bis Security Hub neue Sicherheitsbewertungen generiert, die Daten aus den aktualisierten Regionen enthalten.

Wie werden Sicherheitswerte berechnet

Sicherheitswerte stellen das Verhältnis zwischen bestandenen Kontrollen und aktivierten Kontrollen dar. Die Punktzahl wird als Prozentsatz angezeigt, der auf die nächste ganze Zahl auf- oder abgerundet ist.

Security Hub berechnet eine zusammenfassende Sicherheitsbewertung für alle Ihre aktivierten Standards. Security Hub berechnet auch eine Sicherheitsbewertung für jeden aktivierten Standard. Für die Berechnung der Punktzahl umfassen aktivierte Kontrollen Kontrollen mit dem Status Bestanden, Fehlgeschlagen und Unbekannt. Steuerelemente mit dem Status Keine Daten sind von der Punkteberechnung ausgeschlossen.

Security Hub ignoriert archivierte und unterdrückte Ergebnisse bei der Berechnung des Kontrollstatus. Dies kann sich auf die Sicherheitswerte auswirken. Wenn Sie beispielsweise alle fehlgeschlagenen Ergebnisse für eine Kontrolle unterdrücken, erhält sie den Status Bestanden, was wiederum Ihre Sicherheitswerte verbessern kann. Weitere Informationen zum Kontrollstatus finden Sie unterKonformitätsstatus und Kontrollstatus.

Beispiel für eine Bewertung:

Standard	Kontrollen bestanden	Fehlgeschlagene Kontrollen	Unbekannte Kontrollen	Standardpunktzahl
AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	168	22	0	88%
Benchmark AWS v1.4.0 für GUS-Stiftungen	8	29	0	22%
Benchmark AWS v1.2.0 für GUS-Stiftungen	6	35	0	15%
NIST-Sonderpublikation 800-53 Revision 5	159	56	0	74%
PCI DSS v3.2.1	28	17	0	62%

Bei der Berechnung der zusammenfassenden Sicherheitsbewertung zählt Security Hub jede Kontrolle standardübergreifend nur einmal. Wenn Sie beispielsweise ein Steuerelement aktiviert haben, das für drei aktivierte Standards gilt, zählt es für Bewertungszwecke nur als ein aktiviertes Steuerelement.

In diesem Beispiel beträgt die Gesamtzahl der aktivierten Kontrollen für alle aktivierten Standards zwar 528, Security Hub zählt jedoch jedes einzelne Steuerelement zu Bewertungszwecken nur einmal. Die Anzahl der einzelnen aktivierten Kontrollen liegt wahrscheinlich unter 528. Wenn wir davon ausgehen, dass die Anzahl der eindeutigen aktivierten Kontrollen 515 und die Anzahl der eindeutigen bestandenen Kontrollen 357 beträgt, liegt der Gesamtwert bei 69%. Diese Punktzahl wird berechnet, indem die Anzahl der eindeutigen bestandenen Kontrollen durch die Anzahl der eindeutigen aktivierten Kontrollen dividiert wird.

Möglicherweise haben Sie eine Gesamtpunktzahl, die von der Standardsicherheitsbewertung abweicht, auch wenn Sie in Ihrem Konto in der aktuellen Region nur einen Standard aktiviert

haben. Dies kann der Fall sein, wenn Sie mit einem Administratorkonto angemeldet sind und für Mitgliedskonten zusätzliche Standards oder andere Standards aktiviert sind. Dies kann auch der Fall sein, wenn Sie sich das Ergebnis aus der Aggregationsregion ansehen und zusätzliche Standards oder andere Standards in verknüpften Regionen aktiviert sind.

Sicherheitsbewertungen für Administratorkonten

Wenn Sie mit einem Administratorkonto angemeldet sind, beziehen sich die Sicherheitsbewertung und die Standardwerte auf den Kontrollstatus im Administratorkonto und in allen Mitgliedskonten.

Wenn der Status einer Kontrolle auch nur in einem Mitgliedskonto Fehlgeschlagen lautet, lautet ihr Status im Administratorkonto Fehlgeschlagen und wirkt sich auf die Punktzahlen des Administratorkontos aus.

Wenn Sie mit einem Administratorkonto angemeldet sind und Ergebnisse in einer Aggregationsregion anzeigen, berücksichtigen die Sicherheitsbewertungen den Kontrollstatus in allen Mitgliedskonten und allen verknüpften Regionen.

Sicherheitswerte, wenn Sie eine Aggregationsregion festgelegt haben

Wenn Sie eine Aggregation festgelegt haben AWS-Region, berücksichtigen die zusammenfassende Sicherheitsbewertung und die Standardwerte den Kontrollstatus in allen Bereichen verknüpfte Regionen.

Wenn der Status eines Steuerelements auch nur in einer verknüpften Region Fehlgeschlagen lautet, lautet sein Status in der Aggregationsregion Fehlgeschlagen, was sich auf die Werte der Aggregationsregion auswirkt.

Wenn Sie mit einem Administratorkonto angemeldet sind und sich Punktzahlen in einer Aggregationsregion ansehen, berücksichtigen die Sicherheitsbewertungen den Kontrollstatus in allen Mitgliedskonten und allen verknüpften Regionen.

Referenz zu Security Hub Hub-Standards

AWS Security Hub unterstützt derzeit die in diesem Abschnitt beschriebenen Sicherheitsstandards.

Wählen Sie einen Standard aus, um weitere Informationen zu ihm und den für ihn geltenden Kontrollen zu erhalten.

Die Standards und Kontrollen von Security Hub garantieren nicht die Einhaltung gesetzlicher Rahmenbedingungen oder Audits. Vielmehr bieten die Kontrollen eine Möglichkeit, den aktuellen Status Ihrer Ressourcen AWS-Konten und Ihrer Ressourcen zu überwachen.

Unterstützte Standards

- AWS FSBP-Standard (Basic Security Best Practices)
- CIS AWS Foundations Benchmark
- Nationales Institut für Standards und Technologie (NIST) SP 800-53 Rev. 5
- Payment Card Industry Data Security Standard (PCI DSS)
- AWS Standard für die Kennzeichnung von Ressourcen
- Vom Service verwaltete Standards

AWS FSBP-Standard (Basic Security Best Practices)

Der Standard „Best Practices für AWS grundlegende Sicherheit“ besteht aus einer Reihe von Kontrollen, mit denen festgestellt wird, wenn Sie AWS-Konten und Ihre Ressourcen von den bewährten Sicherheitsmethoden abweichen.

Mit diesem Standard können Sie kontinuierlich all Ihre AWS-Konten Arbeitslasten bewerten, um schnell Bereiche zu identifizieren, in denen Abweichungen von den bewährten Methoden bestehen. Er bietet umsetzbare und verbindliche Leitlinien zur Verbesserung und Aufrechterhaltung der Sicherheitslage in Ihrem Unternehmen.

Die Kontrollen beinhalten bewährte Sicherheitsmethoden für Ressourcen verschiedener Anbieter. AWS-Services Jedem Steuerelement wird außerdem eine Kategorie zugewiesen, die die Sicherheitsfunktion widerspiegelt, für die es gilt. Weitere Informationen finden Sie unter the section called “Kontrollkategorien”.

Kontrollen, die für den FSBP-Standard gelten

[Account.1] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto

[ACM.1] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden

[ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden

[ApiGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein

[ApiGateway.2] API Gateway REST-API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden

[ApiGateway.3] Bei den REST-API-Stufen von API Gateway sollte die Ablaufverfolgung aktiviert sein AWS X-Ray

[ApiGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein

[ApiGateway.5] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden

[ApiGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben

[ApiGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein

[AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben

[AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden

[AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden

[AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken

[AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen

[Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben

[AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden

[AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden

[Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein

Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein

[CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen

[CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein

[CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein

[CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein

[CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden

[CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten

[CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln

[CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden

[CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen

[CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden

[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden

[CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten

[CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten

[CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein

[CodeBuild1.4] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben

[Config.1] AWS Config sollte aktiviert sein

[DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden

[DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein

[DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein

[DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein

[DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein

[DMS.9] DMS-Endpunkte sollten SSL verwenden

[DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein

[DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein

[DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein

[DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden

[DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen

[DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein

[DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch

[DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein

[DynamoDB.1] DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren

[DynamoDB.2] Bei DynamoDB-Tabellen sollte die Wiederherstellung aktiviert sein point-in-time

[DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden

[DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein

[DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden

[EC2.1] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

[EC2.3] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden

[EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein

[EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein

[EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden

[EC2.9] Amazon EC2 EC2-Instances sollten keine öffentliche IPv4-Adresse haben

[EC2.10] Amazon EC2 sollte so konfiguriert sein, dass es VPC-Endpunkte verwendet, die für den Amazon EC2-Service erstellt wurden

[EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen

[EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden

[EC2.17] Amazon EC2 EC2-Instances sollten nicht mehrere ENIs verwenden

[EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen

[EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen

[EC2.20] Beide VPN-Tunnel für eine AWS Site-to-Site-VPN-Verbindung sollten aktiv sein

[EC2.21] Netzwerk-ACLs sollten keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen

[EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren

[EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden

[EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen

[EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein

[ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein

[ECR.2] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein

[ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein

[ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.

[ECS.2] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden

[ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen

[ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden

[ECS.5] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein

[ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden

[ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen

[ECS.10] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen

[ECS.12] ECS-Cluster sollten Container Insights verwenden

[EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS

[EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein

[EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen

[EFS.4] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen

[EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden

[EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein

[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden

[EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden

[EKS.8] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein

[ElastiCache.1] Bei ElastiCache Redis-Clustern sollte das automatische Backup aktiviert sein

[ElastiCache.2] ElastiCache Für Redis-Cache-Cluster sollte das auto Upgrade der Nebenversion aktiviert sein

[ElastiCache.3] ElastiCache Für Redis-Replikationsgruppen sollte der automatische Failover aktiviert sein

[ElastiCache.4] ElastiCache für Redis-Replikationsgruppen sollten im Ruhezustand verschlüsselt werden

[ElastiCache.5] ElastiCache für Redis-Replikationsgruppen sollten bei der Übertragung verschlüsselt werden

[ElastiCache.6] ElastiCache Für Redis-Replikationsgruppen vor Version 6.0 sollte Redis AUTH verwendet werden

[ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden

[ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben

[ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein

[ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch

[ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden

[ELB.2] Classic Load Balancer mit SSL/HTTPS-Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager

[ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden

[ELB.4] Application Load Balancer sollte so konfiguriert sein, dass HTTP-Header gelöscht werden

[ELB.5] Die Protokollierung von Anwendungen und Classic Load Balancers sollte aktiviert sein

[ELB.6] Für Anwendungen, Gateways und Network Load Balancers sollte der Löschschutz aktiviert sein

[ELB.7] Bei Classic Load Balancers sollte der Verbindungsverlust aktiviert sein

[ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config

[ELB.9] Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein

[ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken

[ELB.12] Application Load Balancer sollte mit dem defensiven Modus oder dem strengsten Modus zur Desynchronisierung konfiguriert werden

[ELB.13] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken

[ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden

[EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben

[EMR.2] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein

[ES.1] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein

[ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein

[ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

[ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein

[ES.5] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein

[ES.6] Elasticsearch-Domains sollten mindestens drei Datenknoten haben

[ES.7] Elasticsearch-Domänen sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden

[ES.8] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden

[EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden

[FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden

[FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden

[GuardDuty.1] GuardDuty sollte aktiviert sein

[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen

[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren

[IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen

[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.

[IAM.7] Die Passwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein

[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden

[IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen

[Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden

[KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen

[KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen

[KMS.3] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden

[Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten

[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden

[Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren

[Macie.1] Amazon Macie sollte aktiviert sein

[Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein

[MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch

[MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein

[MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden

[Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden

[Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch

[Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein

[Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein

[Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein

[Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden

[Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein

[Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren

[NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein

[NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben

[NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.

[NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.

[NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein

[NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein

Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein

[Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein

[Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein

Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein

[Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben

Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein

[Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden

Auf [Opensearch.10] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein

[PCA.1] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein

[Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren

[RDS.1] Der RDS-Snapshot sollte privat sein

[RDS.2] RDS-DB-Instances sollten je nach Dauer den öffentlichen Zugriff verbieten PubliclyAccessible AWS Config

[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.

[RDS.4] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden

[RDS.5] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden

[RDS.6] Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden

[RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein

[RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein

[RDS.9] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch

[RDS.10] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden

[RDS.11] Bei RDS-Instances sollten automatische Backups aktiviert sein

[RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden

[RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein

[RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein

[RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden

[RDS.16] RDS-DB-Cluster sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren

[RDS.17] RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren

[RDS.18] RDS-Instances sollten in einer VPC bereitgestellt werden

[RDS.19] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Cluster-Ereignisse konfiguriert werden

[RDS.20] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden

[RDS.21] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden

[RDS.22] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden

[RDS.23] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden

[RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden

[RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden

[RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden

[RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch

[RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein

[Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten

[Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden

[Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein

[Redshift.4] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein

[Redshift.6] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein

[Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden

[Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden

[Redshift.9] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden

[Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden

[Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen

[S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein

[S3.2] S3-Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren

[S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren

[S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern

[S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten

[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren

[S3.9] Bei S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein

[S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten

[S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben

[S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

[SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben

[SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden

[SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben

[SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein

[SecretsManager.1] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein

[SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren

[SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen

[SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden

[ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden

[SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden

[SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager

[SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben

[SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben

[SSM.4] SSM-Dokumente sollten nicht öffentlich sein

[StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben

[Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden

[WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein

[WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben

[WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben

[WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

[WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben

[WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben

[WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

[WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Für [WAF.12] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch

CIS AWS Foundations Benchmark

Der Benchmark der Center for Internet Security (CIS) AWS Foundations dient als Sammlung von bewährten Methoden zur Sicherheitskonfiguration für AWS. Diese branchenweit anerkannten Best Practices bieten Ihnen klare step-by-step Implementierungs- und Bewertungsverfahren. Die Kontrollen in diesem Benchmark reichen von Betriebssystemen über Cloud-Dienste bis hin zu Netzwerkgeräten und helfen Ihnen dabei, die spezifischen Systeme zu schützen, die Ihr Unternehmen verwendet.

AWS Security Hub unterstützt CIS AWS Foundations Benchmark v3.0.0, 1.4.0 und v1.2.0.

Diese Seite listet die Sicherheitskontrollen auf, die jede Version unterstützt, und bietet einen Vergleich der Versionen.

Benchmark AWS v3.0.0 für CIS Foundations

Security Hub unterstützt Version 3.0.0 des CIS AWS Foundations Benchmark.

Security Hub hat die Anforderungen der CIS Security Software Certification erfüllt und wurde mit der CIS Security Software Certification für die folgenden CIS-Benchmarks ausgezeichnet:

- CIS Benchmark for CIS AWS Foundations Benchmark, v3.0.0, Stufe 1
- CIS-Benchmark für AWS GUS-Stiftungen, Benchmark, v3.0.0, Stufe 2

Kontrollen, die für CIS AWS Foundations Benchmark v3.0.0 gelten

[Account.1] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto

[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

[CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist

[Config.1] AWS Config sollte aktiviert sein

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein

[EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein

[EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden

[EC2.21] Netzwerk-ACLs sollten keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen

[EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 zu Remote-Serververwaltungsports zulassen

[EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugang von: :/0 zu Remote-Serveradministrationsports zulassen

[EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS

[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren

[IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen

[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.

[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert

[IAM.16] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert

[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support

[IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden

[IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden

[IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess

[IAM.28] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein

[KMS.4] Die AWS KMS Schlüsselrotation sollte aktiviert sein

[RDS.2] RDS-DB-Instances sollten je nach Dauer den öffentlichen Zugriff verbieten PubliclyAccessible AWS Config

[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.

[RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein

[S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein

[S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern

[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren

[S3.20] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein

[S3.22] S3-Allzweck-Buckets sollten Schreibereignisse auf Objektebene protokollieren

[S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren

CIS AWS Foundations Benchmark v1.4.0

Security Hub unterstützt Version 1.4.0 des CIS AWS Foundations Benchmark.

Kontrollen, die für CIS AWS Foundations Benchmark v1.4.0 gelten

[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden

[CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist

[CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist

[CloudWatch.1] Für den Benutzer „root“ sollten ein Metrik-Logfilter und ein Alarm vorhanden sein

[CloudWatch.4] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für IAM-Richtlinienänderungen vorhanden sind

[CloudWatch1.5] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der Dauer CloudTrail AWS Config vorhanden sind

[CloudWatch.6] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind

[CloudWatch.7] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind

[CloudWatch.8] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind

[CloudWatch.9] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Config Konfigurationsänderungen vorhanden sind

[CloudWatch.10] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind

[CloudWatch.11] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind

[CloudWatch.12] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind

[CloudWatch.13] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind

[CloudWatch.14] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind

[Config.1] AWS Config sollte aktiviert sein

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein

[EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein

[EC2.21] Netzwerk-ACLs sollten keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen

[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren

[IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen

[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.

[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert

[IAM.16] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert

[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support

[IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden

[KMS.4] Die AWS KMS Schlüsselrotation sollte aktiviert sein

[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.

[S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein

[S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern

[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren

[S3.20] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein

Benchmark v1.2.0 der AWS Grundlagen des Zentrums für Internetsicherheit (CIS)

Security Hub unterstützt Version 1.2.0 des CIS AWS Foundations Benchmark.

Security Hub hat die Anforderungen der CIS Security Software Certification erfüllt und wurde mit der CIS Security Software Certification für die folgenden CIS-Benchmarks ausgezeichnet:

- CIS Benchmark for CIS AWS Foundations Benchmark, v1.2.0, Stufe 1
- CIS-Benchmark für AWS GUS-Stiftungen, Benchmark, v1.2.0, Stufe 2

Kontrollen, die für CIS AWS Foundations Benchmark v1.2.0 gelten

[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden

[CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist

[CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist

[CloudWatch.1] Für den Benutzer „root“ sollten ein Metrik-Logfilter und ein Alarm vorhanden sein

[CloudWatch.2] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind

[CloudWatch.3] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Anmeldung an der Management Console ohne MFA vorhanden sind

[CloudWatch.4] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für IAM-Richtlinienänderungen vorhanden sind

[CloudWatch1.5] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der Dauer CloudTrail AWS Config vorhanden sind

[CloudWatch.6] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind

[CloudWatch.7] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind

[CloudWatch.8] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind

[CloudWatch.9] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Config Konfigurationsänderungen vorhanden sind

[CloudWatch.10] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind

[CloudWatch.11] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind

[CloudWatch.12] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind

[CloudWatch.13] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind

[CloudWatch.14] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind

[Config.1] AWS Config sollte aktiviert sein

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein

[EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen

[EC2.14] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulassen

[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen

[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren

[IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen

[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.

[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden

[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

[IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert

[IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert

[IAM.13] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist

[IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert

[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert

[IAM.16] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert

[IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft

[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support

[KMS.4] Die AWS KMS Schlüsselrotation sollte aktiviert sein

Versionsvergleich für CIS AWS Foundations Benchmark

In diesem Abschnitt werden die Unterschiede zwischen den Benchmark v3.0.0, v1.4.0 und v1.2.0 des Center for Internet Security (CIS) AWS Foundations zusammengefasst.

Security Hub unterstützt jede dieser Versionen des CIS AWS Foundations Benchmark, wir empfehlen jedoch, Version 3.0.0 zu verwenden, um über bewährte Sicherheitsmethoden auf dem Laufenden zu bleiben. Möglicherweise haben Sie mehrere Versionen des Standards gleichzeitig aktiviert. Weitere Informationen finden Sie unter Sicherheitsstandards aktivieren und deaktivieren. Wenn Sie ein Upgrade auf v3.0.0 durchführen möchten, aktivieren Sie es am besten zuerst, bevor Sie eine ältere Version deaktivieren. Wenn Sie die Security Hub Hub-Integration mit verwenden AWS Organizations , um mehrere Konten zentral zu verwalten, AWS-Konten und Sie v3.0.0 für alle Konten stapelweise aktivieren möchten, können Sie die zentrale Konfiguration verwenden.

Zuordnung der Kontrollen zu den CIS-Anforderungen in jeder Version

Verstehen Sie, welche Kontrollen jede Version des CIS AWS Foundations Benchmark unterstützt.

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[Account.1] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto	1.2	1.2	1.18
[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst	3.1	3.1	2.1
[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst	3.1	3.1	2.1
[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben	3.5	3.7	2.7
[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein	3.2	3.2	2.2
[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden	Nicht unterstützt — CIS hat diese Anforderung entfernt	3.4	2.4
[CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist	Nicht unterstützt — CIS hat diese Anforderung entfernt	3.3	2.3

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist	3.4	3.6	2.6
[CloudWatch.1] Für den Benutzer „root“ sollten ein Metrik-Logfilter und ein Alarm vorhanden sein	Nicht unterstützt — manuelle Überprüfung	4.3	3.3
[CloudWatch.2] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	3.1
[CloudWatch.3] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Anmeldung an der Management Console ohne MFA vorhanden sind	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	3.2
[CloudWatch.4] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für IAM-Richtlinienänderungen vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.4	3.4
[CloudWatch1.5] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der Dauer CloudTrail AWS Config vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.5	3.5

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[CloudWatch.6] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.6	3.6
[CloudWatch.7] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.7	3.7
[CloudWatch.8] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.8	3.8
[CloudWatch.9] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Config Konfigurationsänderungen vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4,9 bis 4,9	3.9
[CloudWatch.10] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.10	3,10
[CloudWatch.11] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.11	3,11

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[CloudWatch.12] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.12	3,12
[CloudWatch.13] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.13	3.13
[CloudWatch.14] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind	Nicht unterstützt — manuelle Überprüfung	4.14	3,14
[Config.1] AWS Config sollte aktiviert sein	3.3	3.5	2.5
[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen	5.4	5.3	4.3
[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein	3.7	3.9	2,9
[EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein	2.2.1	2.2.1	Nicht unterstützt
[EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden	5.6	Nicht unterstützt	Nicht unterstützt

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen	Nicht unterstützt — ersetzt durch die Anforderungen 5.2 und 5.3	Nicht unterstützt — ersetzt durch die Anforderungen 5.2 und 5.3	4.1
[EC2.14] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulassen	Nicht unterstützt — ersetzt durch die Anforderungen 5.2 und 5.3	Nicht unterstützt — ersetzt durch die Anforderungen 5.2 und 5.3	4.2
[EC2.21] Netzwerk-ACLs sollten keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen	5.1	5.1	Nicht unterstützt
[EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 zu Remote-Serververwaltungsports zulassen	5.2	Nicht unterstützt	Nicht unterstützt
[EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugang von: :/0 zu Remote-Serveradministrationsports zulassen	5.3	Nicht unterstützt	Nicht unterstützt
[EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS	2.4.1	Nicht unterstützt	Nicht unterstützt
[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen	Nicht unterstützt	1.16	1,22
[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein	1.15	Nicht unterstützt	1.16

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden	1.14	1.14	1.4
[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren	1.4	1.4	1.12
[IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen	1.10	1.10	1.2
[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.	1,6	1,6	1.14
[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden	Wird nicht unterstützt — siehe stattdessen [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden	Nicht unterstützt — siehe [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden stattdessen	1.3
[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein	1.5	1.5	1.13
[IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1.5

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1,6
[IAM.13] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1,7
[IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1.8
[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert	1.8	1.8	1.9
[IAM.16] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert	1.9	1.9	1.10
[IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1.11
[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support	1,17	1,17	1.2

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[IAM.20] Vermeiden Sie die Verwendung des Root-Benutzers	Nicht unterstützt — CIS hat diese Anforderung entfernt	Nicht unterstützt — CIS hat diese Anforderung entfernt	1.1
[IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden	1.12	1.12	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden	1.19	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess	1.22	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[IAM.28] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein	1.20	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[KMS.4] Die AWS KMS Schlüsselrotation sollte aktiviert sein	3.6	3.8	2.8

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[Macie.1] Amazon Macie sollte aktiviert sein	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung	Nicht unterstützt — manuelle Überprüfung
[RDS.2] RDS-DB-Instances sollten je nach Dauer den öffentlichen Zugriff verbieten PubliclyAccessible AWS Config	2.3.3	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.	2.3.1	2.3.1	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein	2.3.2	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein	2.1.4	2.1.5	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt

Kontroll-ID und Titel	Anforderung für CIS v3.0.0	CIS v1.4.0-Anforderung	CIS v1.2.0-Anforderung
[S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern	2.1.1	2.1.2	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren	2.1.4	2.1.5	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt
[S3.20] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein	2.1.2	2.1.3	Nicht unterstützt — CIS hat diese Anforderung in späteren Versionen hinzugefügt

ARNs für CIS AWS Foundations Benchmark

Wenn Sie eine oder mehrere Versionen von CIS AWS Foundations Benchmark aktivieren, erhalten Sie die Ergebnisse ab sofort im AWS Security Finding Format (ASFF). In ASFF verwendet jede Version den folgenden Amazon-Ressourcennamen (ARN):

Benchmark AWS v3.0.0 für CIS Foundations

```
arn:aws::securityhub:::standards/cis-aws-foundations-benchmark/v/3.0.0
```

Benchmark v1.4.0 für AWS GUS-Stiftungen

```
arn:aws::securityhub:::standards/cis-aws-foundations-benchmark/v/1.4.0
```

Benchmark v1.2.0 AWS für GUS-Stiftungen

```
arn:aws::securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

Sie können den GetEnabledStandardsBetrieb der Security Hub Hub-API verwenden, um den ARN eines aktivierten Standards herauszufinden.

> **Note**
>
> Wenn Sie eine Version von CIS AWS Foundations Benchmark aktivieren, kann es bis zu 18 Stunden dauern, bis Security Hub Ergebnisse für Kontrollen generiert, die dieselbe AWS Config serviceverknüpfte Regel verwenden wie aktivierte Kontrollen in anderen aktivierten Standards. Weitere Informationen finden Sie unter Zeitplan für die Ausführung von Sicherheitsprüfungen.

Die Suchfelder unterscheiden sich, wenn Sie die Option „Konsolidierte Kontrollergebnisse“ aktivieren. Weitere Informationen zu diesen Unterschieden erhalten Sie unter Auswirkungen der Konsolidierung auf ASFF-Felder und -Werte. Stichprobenergebnisse aus der Kontrolluntersuchung finden Sie unterErgebnisse der Stichprobenkontrolle.

CIS-Anforderungen, die in Security Hub nicht unterstützt werden

Wie in der obigen Tabelle erwähnt, unterstützt Security Hub nicht jede CIS-Anforderung in jeder Version des CIS AWS Foundations Benchmark. Viele der nicht unterstützten Anforderungen können nur manuell bewertet werden, indem der Status Ihrer AWS Ressourcen überprüft wird.

Nationales Institut für Standards und Technologie (NIST) SP 800-53 Rev. 5

NIST SP 800-53 Rev. 5 ist ein Framework für Cybersicherheit und Compliance, das vom National Institute of Standards and Technology (NIST), einer Behörde, die Teil des US-Handelsministeriums ist, entwickelt wurde. Dieses Compliance-Framework hilft Ihnen, die Verfügbarkeit, Vertraulichkeit und Integrität Ihrer Informationssysteme und kritischen Ressourcen zu schützen. US-Bundesbehörden und Auftragnehmer müssen zum Schutz ihrer Systeme die Anforderungen von NIST SP 800-53 einhalten. Private Unternehmen können sie jedoch freiwillig als Leitfaden zur Reduzierung von Cybersicherheitsrisiken verwenden.

Security Hub bietet Steuerungen, die ausgewählte Anforderungen von NIST SP 800-53 unterstützen. Diese Kontrollen werden im Rahmen automatisierter Sicherheitsüberprüfungen bewertet.

Security Hub-Steuerelemente unterstützen keine Anforderungen von NIST SP 800-53, die manuelle Prüfungen erfordern. Darüber hinaus unterstützen Security Hub-Steuerelemente nur die automatisierten NIST SP 800-53-Anforderungen, die in den Details der einzelnen Kontrollen unter Verwandte Anforderungen aufgeführt sind. Wählen Sie ein Steuerelement aus der folgenden Liste aus, um dessen Details zu sehen. Verwandte Anforderungen, die nicht in den Kontrolldetails aufgeführt sind, werden derzeit von Security Hub nicht unterstützt.

Im Gegensatz zu anderen Frameworks schreibt NIST SP 800-53 nicht vor, wie seine Anforderungen bewertet werden sollten. Stattdessen enthält das Framework Richtlinien, und die Security Hub NIST SP 800-53-Steuerelemente stellen das Verständnis dar, das der Service von ihnen hat.

Wenn Sie die Security Hub-Integration mit verwenden AWS Organizations , um mehrere Konten zentral zu verwalten und NIST SP 800-53 für alle Konten stapelweise aktivieren möchten, können Sie vom Administratorkonto aus ein Security Hub-Skript für mehrere Konten ausführen.

Weitere Informationen zu NIST SP 800-53 Rev. 5 finden Sie im NIST Computer Security Resource Center.

Kontrollen, die für NIST SP 800-53 Rev. 5 gelten

[Account.1] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto

[Account.2] AWS-Konten sollte Teil einer Organisation sein AWS Organizations

[ACM.1] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden

[ApiGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein

[ApiGateway.2] API Gateway REST-API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden

[ApiGateway.3] Bei den REST-API-Stufen von API Gateway sollte die Ablaufverfolgung aktiviert sein AWS X-Ray

[ApiGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein

[ApiGateway.5] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden

[ApiGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben

[ApiGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein

[AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden

[AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden

[AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken

[AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen

[Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben

[AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden

[AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden

[Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein

Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein

[CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen

[CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein

[CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein

[CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein

[CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden

[CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten

[CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln

[CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden

[CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen

[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden

[CloudWatch.15] Für CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein

[CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden

[CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein

[CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten

[CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten

[CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein

[CodeBuild1.4] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben

[Config.1] AWS Config sollte aktiviert sein

[DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden

[DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein

[DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein

[DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein

[DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein

[DMS.9] DMS-Endpunkte sollten SSL verwenden

[DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein

[DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein

[DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein

[DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden

[DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen

[DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein

[DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch

[DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein

[DynamoDB.1] DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren

[DynamoDB.2] Bei DynamoDB-Tabellen sollte die Wiederherstellung aktiviert sein point-in-time

[DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden

[DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein

[DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein

[DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden

[EC2.1] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

[EC2.3] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden

[EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein

[EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein

[EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden

[EC2.9] Amazon EC2 EC2-Instances sollten keine öffentliche IPv4-Adresse haben

[EC2.10] Amazon EC2 sollte so konfiguriert sein, dass es VPC-Endpunkte verwendet, die für den Amazon EC2-Service erstellt wurden

[EC2.12] Ungenutzte Amazon EC2 EC2-EIPs sollten entfernt werden

[EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen

[EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen

[EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden

[EC2.17] Amazon EC2 EC2-Instances sollten nicht mehrere ENIs verwenden

[EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen

[EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen

[EC2.20] Beide VPN-Tunnel für eine AWS Site-to-Site-VPN-Verbindung sollten aktiv sein

[EC2.21] Netzwerk-ACLs sollten keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen

[EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren

[EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden

[EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen

[EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden

[EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein

[ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein

[ECR.2] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein

[ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein

[ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.

[ECS.2] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden

[ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen

[ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden

[ECS.5] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein

[ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden

[ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen

[ECS.10] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen

[ECS.12] ECS-Cluster sollten Container Insights verwenden

[EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS

[EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein

[EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen

[EFS.4] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen

[EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden

[EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein

[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden

[EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden

[EKS.8] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein

[ElastiCache.1] Bei ElastiCache Redis-Clustern sollte das automatische Backup aktiviert sein

[ElastiCache.2] ElastiCache Für Redis-Cache-Cluster sollte das auto Upgrade der Nebenversion aktiviert sein

[ElastiCache.3] ElastiCache Für Redis-Replikationsgruppen sollte der automatische Failover aktiviert sein

[ElastiCache.4] ElastiCache für Redis-Replikationsgruppen sollten im Ruhezustand verschlüsselt werden

[ElastiCache.5] ElastiCache für Redis-Replikationsgruppen sollten bei der Übertragung verschlüsselt werden

[ElastiCache.6] ElastiCache Für Redis-Replikationsgruppen vor Version 6.0 sollte Redis AUTH verwendet werden

[ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden

[ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben

[ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein

[ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden

[ELB.2] Classic Load Balancer mit SSL/HTTPS-Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager

[ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden

[ELB.4] Application Load Balancer sollte so konfiguriert sein, dass HTTP-Header gelöscht werden

[ELB.5] Die Protokollierung von Anwendungen und Classic Load Balancers sollte aktiviert sein

[ELB.6] Für Anwendungen, Gateways und Network Load Balancers sollte der Löschschutz aktiviert sein

[ELB.7] Bei Classic Load Balancers sollte der Verbindungsverlust aktiviert sein

[ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config

[ELB.9] Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein

[ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken

[ELB.12] Application Load Balancer sollte mit dem defensiven Modus oder dem strengsten Modus zur Desynchronisierung konfiguriert werden

[ELB.13] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken

[ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden

[ELB.16] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF

[EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben

[EMR.2] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein

[ES.1] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein

[ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein

[ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

[ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein

[ES.5] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein

[ES.6] Elasticsearch-Domains sollten mindestens drei Datenknoten haben

[ES.7] Elasticsearch-Domänen sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden

[ES.8] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden

[EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden

[EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein

[FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden

[FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden

[GuardDuty.1] GuardDuty sollte aktiviert sein

[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen

[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren

[IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen

[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.

[IAM.7] Die Passwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein

[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden

[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

[IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein

[IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen

[Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden

[KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen

[KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen

[KMS.3] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden

[KMS.4] Die AWS KMS Schlüsselrotation sollte aktiviert sein

[Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten

[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden

[Lambda.3] Lambda-Funktionen sollten sich in einer VPC befinden

[Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren

[Macie.1] Amazon Macie sollte aktiviert sein

[Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein

[MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden

[MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein

[MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch

[MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein

[MQ.5] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden

[MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden

[Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden

[Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch

[Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein

[Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein

[Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein

[Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden

[Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein

[Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren

[Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden

[NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden

[NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein

[NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben

[NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.

[NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.

[NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein

[NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein

Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein

[Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein

[Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein

Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein

[Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben

Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein

[Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden

Auf [Opensearch.10] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein

[Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben

[PCA.1] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein

[RDS.1] Der RDS-Snapshot sollte privat sein

[RDS.2] RDS-DB-Instances sollten je nach Dauer den öffentlichen Zugriff verbieten PubliclyAccessible AWS Config

[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.

[RDS.4] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden

[RDS.5] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden

[RDS.6] Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden

[RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein

[RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein

[RDS.9] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch

[RDS.10] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden

[RDS.11] Bei RDS-Instances sollten automatische Backups aktiviert sein

[RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden

[RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein

[RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein

[RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden

[RDS.16] RDS-DB-Cluster sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren

[RDS.17] RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren

[RDS.18] RDS-Instances sollten in einer VPC bereitgestellt werden

[RDS.19] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Cluster-Ereignisse konfiguriert werden

[RDS.20] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden

[RDS.21] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden

[RDS.22] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden

[RDS.23] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden

[RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden

[RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden

[RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden

[RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden

[RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch

[RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein

[Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten

[Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden

[Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein

[Redshift.4] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein

[Redshift.6] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein

[Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden

[Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden

[Redshift.9] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden

[Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden

[Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren

[S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein

[S3.2] S3-Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren

[S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren

[S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern

[S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten

[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden

[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren

[S3.9] Bei S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein

[S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben

[S3.11] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein

[S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten

[S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben

[S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein

[S3.15] Bei S3-Allzweck-Buckets sollte Object Lock aktiviert sein

[S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys

[S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

[S3.20] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein

[SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben

[SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden

[SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben

[SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein

[SecretsManager.1] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein

[SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren

[SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen

[SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden

[ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden

[SNS.1] SNS-Themen sollten im Ruhezustand wie folgt verschlüsselt werden AWS KMS

[SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden

[SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager

[SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben

[SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben

[SSM.4] SSM-Dokumente sollten nicht öffentlich sein

[Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden

[WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein

[WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben

[WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben

[WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

[WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben

[WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben

[WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

[WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

[WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein

Für [WAF.12] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch

Payment Card Industry Data Security Standard (PCI DSS)

Der Payment Card Industry Data Security Standard (PCI DSS) in Security Hub bietet eine Reihe von bewährten AWS Sicherheitsmethoden für den Umgang mit Karteninhaberdaten. Sie können diesen

Standard verwenden, um Sicherheitslücken in Ressourcen zu entdecken, die Karteninhaberdaten verarbeiten. Security Hub umfasst derzeit die Kontrollen auf Kontoebene. Wir empfehlen Ihnen, diese Kontrollen für all Ihre Konten zu aktivieren, die über Ressourcen verfügen, die Karteninhaberdaten speichern, verarbeiten oder übertragen.

Dieser Standard wurde von AWS Security Assurance Services LLC (AWS SAS), einem Team qualifizierter Sicherheitsgutachter (QSAs), das für die Bereitstellung von PCI-DSS-Leitlinien zertifiziert ist, sowie von Bewertungen durch das PCI DSS Security Standards Council (PCI SSC) validiert. AWS SAS hat bestätigt, dass die automatisierten Prüfungen Kunden bei der Vorbereitung auf eine PCI DSS-Bewertung unterstützen können.

Auf dieser Seite sind die IDs und Titel der Sicherheitskontrollen aufgeführt. In den Regionen AWS GovCloud (US) Region und China werden standardspezifische Kontroll-IDs und Titel verwendet. Eine Zuordnung von IDs und Titeln für Sicherheitskontrollen zu standardspezifischen Kontroll-IDs und Titeln finden Sie unter. Wie sich die Konsolidierung auf Kontroll-IDs und Titel auswirkt

Kontrollen, die für PCI DSS gelten

[AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

[CloudTrail.3] Mindestens ein CloudTrail Trail sollte aktiviert sein

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden

[CloudWatch.1] Für den Benutzer „root“ sollten ein Metrik-Logfilter und ein Alarm vorhanden sein

[CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten

[CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten

[Config.1] AWS Config sollte aktiviert sein

[DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein

[EC2.1] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein

[EC2.12] Ungenutzte Amazon EC2 EC2-EIPs sollten entfernt werden

[EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen

[ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden

[ES.1] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein

[ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein

[GuardDuty.1] GuardDuty sollte aktiviert sein

[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen

[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren

[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.

[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden

[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

[IAM.10] Passwortrichtlinien für IAM-Benutzer sollten strenge Laufzeiten haben AWS Config

[IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein

[KMS.4] Die AWS KMS Schlüsselrotation sollte aktiviert sein

[Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten

[Lambda.3] Lambda-Funktionen sollten sich in einer VPC befinden

Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein

[Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein

[RDS.1] Der RDS-Snapshot sollte privat sein

[RDS.2] RDS-DB-Instances sollten je nach Dauer den öffentlichen Zugriff verbieten PubliclyAccessible AWS Config

[Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten

[S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein

[S3.2] S3-Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren

[S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren

[S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern

[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden

[SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben

[SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager

[SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben

[SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben

AWS Standard für die Kennzeichnung von Ressourcen

Dieser Abschnitt enthält Informationen zum AWS Resource Tagging Standard.

> **Note**
>
> Der AWS Resource Tagging Standard ist in Kanada West (Calgary), China und nicht verfügbar. AWS GovCloud (US)

Was ist der AWS Resource Tagging Standard?

Tags sind Schlüssel- und Wertepaare, die als Metadaten für die Organisation Ihrer AWS Ressourcen dienen. Bei den meisten AWS Ressourcen haben Sie die Möglichkeit, Tags bei der Erstellung der Ressource oder nach der Erstellung hinzuzufügen. Zu den Ressourcen gehören beispielsweise eine

CloudFront Amazon-Distribution, eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance oder ein Secret In AWS Secrets Manager.

Mit Tags können Sie Ressourcen verwalten, identifizieren, organisieren, suchen und filtern.

Jedes Tag besteht aus zwei Teilen:

- einem Tag-Schlüssel (z. B. `CostCenter`, `Environment` oder `Project`). Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.
- Ein Tag-Wert (zum Beispiel `111122223333` oder`Production`). Wie bei Tag-Schlüsseln wird auch bei Tag-Werten zwischen Groß- und Kleinschreibung unterschieden.

Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren.

Anweisungen zum Hinzufügen von Tags zu AWS Ressourcen finden Sie unter So fügen Sie Ihrer AWS Ressource Tags hinzu im AWS Security Hub Hub-Benutzerhandbuch.

Mit dem von AWS Security Hub entwickelten AWS Resource Tagging Standard können Sie schnell feststellen, ob bei einer Ihrer AWS Ressourcen Tagschlüssel fehlen. Sie können den `requiredTagKeys` Parameter anpassen, um bestimmte Tag-Schlüssel anzugeben, nach denen die Steuerelemente suchen. Wenn bestimmte Tags nicht bereitgestellt werden, prüfen die Steuerelemente lediglich, ob mindestens ein Tag-Schlüssel vorhanden ist.

Wenn Sie den AWS Resource Tagging Standard aktivieren, erhalten Sie ab sofort Ergebnisse im AWS Security Finding Format (ASFF).

> **Note**
>
> Wenn Sie AWS Resource Tagging Standard aktivieren, kann es bis zu 18 Stunden dauern, bis Security Hub Ergebnisse für Kontrollen generiert, die dieselbe AWS Config serviceverknüpfte Regel verwenden wie aktivierte Steuerelemente in anderen aktivierten Standards. Weitere Informationen finden Sie unter Zeitplan für die Ausführung von Sicherheitsprüfungen.

Dieser Standard hat den folgenden Amazon-Ressourcennamen (ARN):`arn:aws:securityhub:`*`region`*`::standards/aws-resource-tagging-standard/v/1.0.0`.

Sie können auch den GetEnabledStandardsBetrieb der Security Hub Hub-API verwenden, um den ARN eines aktivierten Standards herauszufinden.

Kontrollen im AWS Resource Tagging Standard

Der AWS Resource Tagging Standard umfasst die folgenden Steuerelemente. Wählen Sie ein Steuerelement aus, um eine detaillierte Beschreibung des Steuerelements anzuzeigen.

- [ACM.3] ACM-Zertifikate sollten mit einem Tag versehen werden
- [AppSync.4] AWS AppSync GraphQL-APIs sollten markiert werden
- [Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden
- [Athena.3] Athena-Arbeitsgruppen sollten markiert werden
- [AutoScaling.10] EC2 Auto Scaling Scaling-Gruppen sollten markiert werden
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.3] AWS Backup Tresore sollten markiert sein
- [Backup.4] AWS Backup Berichtspläne sollten markiert werden
- [Backup.5] AWS Backup Backup-Pläne sollten markiert werden
- [CloudFormation.2] CloudFormation Stapel sollten markiert werden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CloudTrail.9] CloudTrail Pfade sollten markiert werden
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [Detective.1] Verhaltensdiagramme von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten gekennzeichnet sein
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DynamoDB.5] DynamoDB-Tabellen sollten mit Tags versehen werden
- [EC2.33] EC2 Transit Gateway-Anhänge sollten markiert werden
- [EC2.34] Die Routentabellen des EC2-Transit-Gateways sollten mit Tags versehen werden
- [EC2.35] EC2-Netzwerkschnittstellen sollten markiert werden
- [EC2.36] EC2-Kunden-Gateways sollten mit Tags versehen werden
- [EC2.37] EC2-Elastic-IP-Adressen sollten mit Tags versehen werden

- [EC2.38] EC2-Instances sollten markiert werden
- [EC2.39] EC2-Internet-Gateways sollten markiert werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.41] EC2-Netzwerk-ACLs sollten markiert werden
- [EC2.42] EC2-Routing-Tabellen sollten mit Tags versehen werden
- [EC2.43] EC2-Sicherheitsgruppen sollten markiert werden
- [EC2.44] EC2-Subnetze sollten markiert werden
- [EC2.45] EC2-Volumes sollten markiert werden
- [EC2.46] Amazon VPCs sollten markiert werden
- [EC2.47] Amazon VPC Endpoint Services sollten markiert werden
- [EC2.48] Amazon VPC-Flow-Logs sollten markiert werden
- [EC2.49] Amazon VPC-Peering-Verbindungen sollten markiert werden
- [EC2.50] EC2-VPN-Gateways sollten markiert werden
- [EC2.52] EC2-Transit-Gateways sollten markiert werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECS.13] ECS-Services sollten markiert werden
- [ECS.14] ECS-Cluster sollten markiert werden
- [ECS.15] ECS-Aufgabendefinitionen sollten mit Tags versehen werden
- [EFS.5] EFS-Zugangspunkte sollten markiert werden
- [EKS.6] EKS-Cluster sollten markiert werden
- [EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden
- [ES.9] Elasticsearch-Domains sollten markiert werden
- [EventBridge.2] EventBridge Eventbusse sollten gekennzeichnet sein
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [Glue.1] AWS Glue Jobs sollten markiert werden
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen werden
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [IAM.23] IAM Access Analyzer-Analyzer sollten markiert werden

- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden
- [IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden
- [IoT.3] AWS IoT Core -Dimensionen sollten markiert werden
- [IoT.4] AWS IoT Core Autorisierer sollten markiert werden
- [IoT.5] AWS IoT Core Rollenaliase sollten markiert werden
- [IoT.6] AWS IoT Core Richtlinien sollten markiert werden
- [Kinesis.2] Kinesis-Streams sollten markiert werden
- [Lambda.6] Lambda-Funktionen sollten markiert werden
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [NetworkFirewall.7] Netzwerk-Firewall-Firewalls sollten markiert werden
- [NetworkFirewall.8] Firewall-Richtlinien für Netzwerk-Firewalls sollten markiert werden
- [Opensearch.9] OpenSearch -Domains sollten mit Tags versehen werden
- [RDS.28] RDS-DB-Cluster sollten markiert werden
- [RDS.29] RDS-DB-Cluster-Snapshots sollten mit Tags versehen werden
- [RDS.30] RDS-DB-Instances sollten markiert werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.32] RDS-DB-Snapshots sollten markiert werden
- [RDS.33] RDS-DB-Subnetzgruppen sollten markiert werden
- [Redshift.11] Redshift-Cluster sollten markiert werden
- [Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden
- [Redshift.13] Redshift-Cluster-Snapshots sollten markiert werden
- [Redshift.14] Redshift-Cluster-Subnetzgruppen sollten markiert werden
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [SecretsManager.5] Secrets Manager Manager-Geheimnisse sollten markiert werden
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SNS.3] SNS-Themen sollten markiert werden

- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [StepFunctions.2] Die Aktivitäten von Step Functions sollten markiert werden
- [Transfer.1] AWS Transfer Family -Workflows sollten mit Tags versehen werden

Vom Service verwaltete Standards

Ein vom Service verwalteter Standard ist ein Sicherheitsstandard, der von einem anderen AWS-Service verwaltet wird. Zum Beispiel ist Service-Managed Standard: ein vom Service verwalteter Standard, der verwaltet AWS Control Tower wird. AWS Control Tower Ein Service-Managed-Standard unterscheidet sich von einem Sicherheitsstandard, den AWS Security Hub auf folgende Weise verwaltet:

- Erstellung und Löschung von Standards — Sie erstellen und löschen einen vom Service verwalteten Standard mit der Konsole oder API des verwaltenden Dienstes oder mit dem. AWS CLI Solange Sie den Standard nicht auf eine dieser Arten im Verwaltungsdienst erstellt haben, wird der Standard nicht in der Security Hub Hub-Konsole angezeigt und ist nicht über die Security Hub Hub-API oder zugänglich AWS CLI.
- Keine automatische Aktivierung von Kontrollen — Wenn Sie einen vom Service verwalteten Standard erstellen, aktivieren Security Hub und der Verwaltungsdienst nicht automatisch die Kontrollen, die für den Standard gelten. Wenn Security Hub neue Steuerelemente für den Standard veröffentlicht, werden diese außerdem nicht automatisch aktiviert. Dies ist eine Abkehr von den Standards, die Security Hub verwaltet. Weitere Informationen zur üblichen Konfiguration von Steuerelementen in Security Hub finden Sie unterSicherheitskontrollen anzeigen und verwalten.
- Steuerungen aktivieren und deaktivieren — Wir empfehlen, die Steuerungen im Verwaltungsdienst zu aktivieren und zu deaktivieren, um Abweichungen zu vermeiden.
- Verfügbarkeit von Kontrollen — Der Verwaltungsdienst entscheidet, welche Kontrollen im Rahmen des vom Service verwalteten Standards verfügbar sind. Die verfügbaren Kontrollen können alle oder einen Teil der vorhandenen Security Hub-Steuerelemente umfassen.

Nachdem der verwaltende Dienst den vom Service verwalteten Standard erstellt und Kontrollen dafür verfügbar gemacht hat, können Sie in der Security Hub-Konsole, der Security Hub-API oder auf Ihre Kontrollergebnisse, Kontrollstatus und Standardsicherheitsbewertung zugreifen. AWS CLI Einige oder alle dieser Informationen sind möglicherweise auch im Verwaltungsdienst verfügbar.

Wählen Sie einen vom Service verwalteten Standard aus der folgenden Liste aus, um weitere Informationen zu diesem Standard zu erhalten.

Vom Service verwaltete Standards

- Vom Service verwalteter Standard: AWS Control Tower

Vom Service verwalteter Standard: AWS Control Tower

Dieser Abschnitt enthält Informationen zum Service-Managed Standard: AWS Control Tower.

Was ist Service-Managed Standard:? AWS Control Tower

Dieser Standard richtet sich an Benutzer von AWS Security Hub und AWS Control Tower. Damit können Sie die proaktiven Kontrollen AWS Control Tower neben den detektiven Kontrollen von Security Hub im AWS Control Tower Service konfigurieren.

Proaktive Kontrollen tragen dazu bei, dass Sie die Vorschriften AWS-Konten einhalten, da sie Aktionen kennzeichnen, die zu Richtlinienverstößen oder Fehlkonfigurationen führen können. Detective Controls erkennt die Nichtkonformität von Ressourcen (z. B. Fehlkonfigurationen) in Ihrem. AWS-Konten Indem Sie proaktive und detektive Kontrollen für Ihre AWS Umgebung aktivieren, können Sie Ihre Sicherheitslage in verschiedenen Entwicklungsphasen verbessern.

> **Tip**
>
> Von Services verwaltete Standards unterscheiden sich von den Standards, die AWS Security Hub verwaltet. Beispielsweise müssen Sie im Verwaltungsdienst einen vom Dienst verwalteten Standard erstellen und löschen. Weitere Informationen finden Sie unter Vom Service verwaltete Standards.

In der Security Hub Hub-Konsole und der API können Sie Service-Managed Standard: AWS Control Tower neben anderen Security Hub Hub-Standards anzeigen.

Den Standard erstellen

Dieser Standard ist nur verfügbar, wenn Sie den Standard in erstellen AWS Control Tower. AWS Control Tower erstellt den Standard, wenn Sie ein entsprechendes Steuerelement zum ersten Mal mithilfe einer der folgenden Methoden aktivieren:

- AWS Control Tower Konsole
- AWS Control Tower API (rufen Sie die `EnableControl`API auf)
- AWS CLI (führe den `enable-control`Befehl aus)

Security Hub-Steuerelemente werden in der AWS Control Tower Konsole als SH identifiziert. ***ControlID*** (zum Beispiel SH). CodeBuild.1).

Wenn Sie den Standard erstellen und Security Hub noch nicht aktiviert haben, wird Security Hub AWS Control Tower auch für Sie aktiviert.

Wenn Sie ihn nicht eingerichtet haben AWS Control Tower, können Sie diesen Standard in der Security Hub-Konsole, der Security Hub-API oder nicht anzeigen oder darauf zugreifen AWS CLI. Selbst wenn Sie ihn eingerichtet haben AWS Control Tower, können Sie diesen Standard in Security Hub nicht anzeigen oder darauf zugreifen, ohne den Standard zuerst AWS Control Tower mit einer der oben genannten Methoden zu erstellen.

Dieser Standard ist nur dort verfügbar, AWS-Regionen wo er verfügbar AWS Control Tower ist, einschließlich AWS GovCloud (US).

Steuerungen im Standard aktivieren und deaktivieren

Nachdem Sie den Standard in der AWS Control Tower Konsole erstellt haben, können Sie den Standard und die verfügbaren Steuerelemente in beiden Diensten anzeigen.

Nachdem Sie den Standard zum ersten Mal erstellt haben, enthält er keine Steuerelemente, die automatisch aktiviert werden. Wenn Security Hub neue Steuerelemente hinzufügt, werden diese außerdem nicht automatisch für Service-Managed Standard: AWS Control Tower aktiviert. Sie sollten die Steuerelemente für den Standard in aktivieren und deaktivieren, AWS Control Tower indem Sie eine der folgenden Methoden verwenden:

- AWS Control Tower Konsole
- AWS Control Tower API (rufen Sie die `DisableControl`APIs `EnableControl`und auf)
- AWS CLI (führe die `disable-control`Befehle `enable-control`und aus)

Wenn Sie den Aktivierungsstatus eines Steuerelements in ändern AWS Control Tower, wird die Änderung auch in Security Hub widergespiegelt.

Die Deaktivierung eines Steuerelements in Security Hub, das aktiviert ist, AWS Control Tower führt jedoch zu Kontrollabweichungen. Der Kontrollstatus in AWS Control Tower wird als `Drifted` angezeigt. Sie können diese Abweichung beheben, indem Sie in der AWS Control Tower Konsole die Option OU erneut registrieren auswählen oder die Steuerung AWS Control Tower mithilfe einer der oben genannten Methoden deaktivieren und erneut aktivieren.

Wenn Sie die Aktivierungs- und Deaktivierungsaktionen in abschließen, können Sie Kontrollabweichungen vermeiden. AWS Control Tower

Wenn Sie Kontrollen in aktivieren oder deaktivieren AWS Control Tower, gilt die Aktion für alle Konten und Regionen. Wenn Sie Steuerungen in Security Hub aktivieren und deaktivieren (für diesen Standard nicht empfohlen), gilt die Aktion nur für das aktuelle Konto und die Region.

> **Note**
>
> Die zentrale Konfiguration kann nicht zur Verwaltung von Service-Managed Standard: AWS Control Tower verwendet werden. Wenn Sie die zentrale Konfiguration verwenden, können Sie nur den AWS Control Tower Dienst verwenden, um die Steuerungen in diesem Standard für ein zentral verwaltetes Konto zu aktivieren und zu deaktivieren.

Aktivierungsstatus und Kontrollstatus anzeigen

Sie können den Aktivierungsstatus einer Kontrolle mit einer der folgenden Methoden anzeigen:

- Security Hub Hub-Konsole, Security Hub Hub-API oder AWS CLI
- AWS Control Tower Konsole
- AWS Control Tower API, um eine Liste der aktivierten Steuerelemente zu sehen (rufen Sie die `ListEnabledControls`API auf)
- AWS CLI um eine Liste der aktivierten Steuerelemente zu sehen (führen Sie den `list-enabled-controls`Befehl aus)

Ein Steuerelement, das Sie deaktivieren, AWS Control Tower hat den Aktivierungsstatus `Disabled` in Security Hub, sofern Sie dieses Steuerelement nicht ausdrücklich in Security Hub aktivieren.

Security Hub berechnet den Kontrollstatus auf der Grundlage des Workflow-Status und des Compliance-Status der Kontrollergebnisse. Weitere Informationen zum Aktivierungsstatus und zum Kontrollstatus finden Sie unter. Details für ein Steuerelement anzeigen

Auf der Grundlage des Kontrollstatus berechnet Security Hub eine Sicherheitsbewertung für Service-Managed Standard:. AWS Control Tower Diese Bewertung ist nur in Security Hub verfügbar. Darüber hinaus können Sie Kontrollergebnisse nur in Security Hub anzeigen. Die Standardsicherheitsbewertung und die Kontrollergebnisse sind in nicht verfügbar AWS Control Tower.

> **Note**
>
> Wenn Sie Kontrollen für Service-Managed Standard: aktivieren AWS Control Tower, kann es bis zu 18 Stunden dauern, bis Security Hub Ergebnisse für Kontrollen generiert, die eine bestehende AWS Config serviceverknüpfte Regel verwenden. Möglicherweise verfügen Sie bereits über serviceverknüpfte Regeln, wenn Sie andere Standards und Kontrollen in Security Hub aktiviert haben. Weitere Informationen finden Sie unter Zeitplan für die Ausführung von Sicherheitsprüfungen.

Den Standard löschen

Sie können diesen Standard löschen, AWS Control Tower indem Sie alle entsprechenden Steuerelemente mit einer der folgenden Methoden deaktivieren:

- AWS Control Tower Konsole
- AWS Control Tower API (rufen Sie die `DisableControl`API auf)
- AWS CLI (führe den `disable-control`Befehl aus)

Durch das Deaktivieren aller Steuerelemente wird der Standard in allen verwalteten Konten und kontrollierten Regionen in gelöscht. AWS Control Tower Wenn Sie den Standard-in löschen, wird er von der Seite Standards der Security Hub Hub-Konsole AWS Control Tower entfernt, und Sie können nicht mehr über die Security Hub Hub-API oder darauf zugreifen AWS CLI.

> **Note**
>
> Wenn Sie alle Steuerelemente aus dem Standard in Security Hub deaktivieren, wird der Standard nicht deaktiviert oder gelöscht.

Durch die Deaktivierung des Security Hub Hub-Dienstes werden Service-Managed Standard: AWS Control Tower und alle anderen Standards, die Sie aktiviert haben, entfernt.

Das Feldformat für Service-Managed Standard finden: AWS Control Tower

Wenn Sie Service-Managed Standard: erstellen AWS Control Tower und Kontrollen dafür aktivieren, erhalten Sie ab sofort Kontrollergebnisse in Security Hub. Security Hub meldet Kontrollergebnisse in

derAWS Format für Sicherheitssuche (ASFF). Dies sind die ASFF-Werte für den Amazon Resource Name (ARN) dieses Standards und`GeneratorId`:

- Standard-ARN — *`arn:aws:us-east-1`*`:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0`
- GeneratorId – `service-managed-aws-control-tower/v/1.0.0/`*`CodeBuild.1`*

Ein Beispiel für einen Befund für Service-Managed Standard: finden Sie AWS Control Tower unterErgebnisse der Stichprobenkontrolle.

Kontrollen, die für Service-Managed Standard gelten: AWS Control Tower

Service-Managed Standard: AWS Control Tower unterstützt eine Teilmenge von Kontrollen, die Teil des FSBP-Standards (AWS Foundational Security Best Practices) sind. Wählen Sie ein Steuerelement aus der folgenden Tabelle aus, um Informationen dazu anzuzeigen, einschließlich der Schritte zur Behebung fehlgeschlagener Ergebnisse.

Die folgende Liste zeigt die verfügbaren Steuerelemente für Service-Managed Standard:. AWS Control Tower Die regionalen Grenzwerte für Kontrollen entsprechen den regionalen Grenzwerten für die entsprechenden Kontrollen im FSBP-Standard. Diese Liste enthält standardunabhängige IDs für Sicherheitskontrollen. In der AWS Control Tower Konsole sind die Kontroll-IDs als SH formatiert. ***`ControlID (`***zum Beispiel SH). CodeBuild.1). Wenn in Security Hub konsolidierte Kontrollergebnisse in Ihrem Konto deaktiviert sind, verwendet das `ProductFields.ControlId` Feld die standardbasierte Kontroll-ID. Die standardbasierte Kontroll-ID ist als CT formatiert. ***`ControlId`***(zum Beispiel CT. CodeBuild.1).

- [Account.1] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto
- [ACM.1] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [ApiGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein
- [ApiGateway.2] API Gateway REST-API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [ApiGateway.3] Bei den REST-API-Stufen von API Gateway sollte die Ablaufverfolgung aktiviert sein AWS X-Ray

- [ApiGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein
- [ApiGateway.5] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden
- [ApiGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben
- [ApiGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden
- [AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken
- [AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen
- [Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben
- [AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden
- [AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden
- [CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst
- [CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben
- [CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein
- [CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden
- [CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild1.4] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben

- [DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DynamoDB.1] DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren
- [DynamoDB.2] Bei DynamoDB-Tabellen sollte die Wiederherstellung aktiviert sein point-in-time
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [EC2.1] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein
- [EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen
- [EC2.3] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein
- [EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein
- [EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.9] Amazon EC2 EC2-Instances sollten keine öffentliche IPv4-Adresse haben
- [EC2.10] Amazon EC2 sollte so konfiguriert sein, dass es VPC-Endpunkte verwendet, die für den Amazon EC2-Service erstellt wurden
- [EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen
- [EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden
- [EC2.17] Amazon EC2 EC2-Instances sollten nicht mehrere ENIs verwenden
- [EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen
- [EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen
- [EC2.20] Beide VPN-Tunnel für eine AWS Site-to-Site-VPN-Verbindung sollten aktiv sein

- [EC2.21] Netzwerk-ACLs sollten keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen
- [EC2.22] Ungenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.
- [ECS.2] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden
- [ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen
- [ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden
- [ECS.5] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein
- [ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden
- [ECS.10] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen
- [ECS.12] ECS-Cluster sollten Container Insights verwenden
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen
- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [ElastiCache.3] ElastiCache Für Redis-Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache für Redis-Replikationsgruppen sollten im Ruhezustand verschlüsselt werden

- [ElastiCache.5] ElastiCache für Redis-Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache Für Redis-Replikationsgruppen vor Version 6.0 sollte Redis AUTH verwendet werden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden
- [ELB.2] Classic Load Balancer mit SSL/HTTPS-Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden
- [ELB.4] Application Load Balancer sollte so konfiguriert sein, dass HTTP-Header gelöscht werden
- [ELB.5] Die Protokollierung von Anwendungen und Classic Load Balancers sollte aktiviert sein
- [ELB.6] Für Anwendungen, Gateways und Network Load Balancers sollte der Löschschutz aktiviert sein
- [ELB.7] Bei Classic Load Balancers sollte der Verbindungsverlust aktiviert sein
- [ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config
- [ELB.9] Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein
- [ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken
- [ELB.12] Application Load Balancer sollte mit dem defensiven Modus oder dem strengsten Modus zur Desynchronisierung konfiguriert werden
- [ELB.13] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [ES.1] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein

- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein
- [ES.5] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein
- [ES.6] Elasticsearch-Domains sollten mindestens drei Datenknoten haben
- [ES.7] Elasticsearch-Domänen sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden
- [ES.8] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen
- [IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.
- [IAM.7] Die Passwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.3] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden
- [KMS.4] Die AWS KMS Schlüsselrotation sollte aktiviert sein
- [Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten
- [Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden

- [Lambda.3] Lambda-Funktionen sollten sich in einer VPC befinden
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MQ.5] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein
- Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben
- Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein

- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.2] RDS-DB-Instances sollten je nach Dauer den öffentlichen Zugriff verbieten PubliclyAccessible AWS Config
- [RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.
- [RDS.4] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden
- [RDS.5] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden
- [RDS.6] Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden
- [RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein
- [RDS.9] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.10] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden
- [RDS.11] Bei RDS-Instances sollten automatische Backups aktiviert sein
- [RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden
- [RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein
- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.17] RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [RDS.18] RDS-Instances sollten in einer VPC bereitgestellt werden
- [RDS.19] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Cluster-Ereignisse konfiguriert werden
- [RDS.20] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden
- [RDS.21] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden
- [RDS.22] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden
- [RDS.23] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden
- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden

- [Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten
- [Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden
- [Redshift.4] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein
- [Redshift.6] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein
- [Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden
- [Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden
- [Redshift.9] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein
- [S3.2] S3-Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren
- [S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren
- [S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern
- [S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten
- [S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren
- [S3.9] Bei S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein
- [S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten
- [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben
- [S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SecretsManager.1] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein
- [SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren

- [SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen
- [SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden
- [SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Weitere Informationen zu diesem Standard finden Sie unter Security Hub-Steuerelemente im AWS Control Tower Benutzerhandbuch.

Sicherheitsstandards anzeigen und verwalten

Sicherheitsstandards umfassen eine Reihe von Anforderungen, anhand derer die Einhaltung gesetzlicher Rahmenbedingungen, branchenüblicher Best Practices oder Unternehmensrichtlinien überprüft werden kann. AWS Security Hub ordnet diese Anforderungen den Kontrollen zu und führt Sicherheitsüberprüfungen der Kontrollen durch, um zu beurteilen, ob die Anforderungen einer Norm erfüllt werden. Eine Kontrolle kann in einem oder mehreren Standards aktiviert werden. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, generiert Security Hub ein einziges Ergebnis pro Sicherheitsprüfung, auch wenn eine Kontrolle Teil mehrerer aktivierter Standards ist. Weitere Informationen finden Sie unter Konsolidierte Kontrollergebnisse.

Eine Liste der verfügbaren Standards und der für sie geltenden Kontrollen finden Sie unterReferenz zu Standards. Auf der Seite Sicherheitsstandards auf der Security Hub-Konsole werden auch alle unterstützten Sicherheitsstandards in Security Hub und deren Aktivierungsstatus angezeigt. Für jeden Sicherheitsstandard, der in Ihrem Konto aktiviert ist (oder, wenn Sie die Integration mit verwenden

AWS Organizations, in mindestens einem Konto in Ihrer Organisation), können Sie die folgenden Informationen einsehen:

- Der Aktivierungsstatus des Standards in verschiedenen Security Hub Hub-Konfigurationsrichtlinien, wenn Sie die zentrale Konfiguration verwenden
- Eine Beschreibung aller deaktivierten Standards
- Eine Liste der Kontrollen, die derzeit im Standard aktiviert sind, und der Gesamtstatus dieser Kontrollen auf der Grundlage des Konformitätsstatus ihrer Ergebnisse
- eine Liste der Kontrollen, die für den Standard gelten, aber derzeit deaktiviert sind
- Eine Sicherheitsbewertung für den Standard

Security Hub generiert für jeden Standard eine Sicherheitsbewertung. Administratorkonten sehen aggregierte Sicherheitsbewertungen und kontrollieren den Status aller Mitgliedskonten. Wenn Sie eine Aggregationsregion festgelegt haben, spiegeln Ihre Sicherheitswerte den Konformitätsstatus der Kontrollen in allen verknüpften Regionen wider. Weitere Informationen finden Sie unter Wie werden Sicherheitswerte berechnet.

Themen

- Sicherheitsstandards aktivieren und deaktivieren
- Details für einen Standard anzeigen
- Steuerungen in bestimmten Standards aktivieren und deaktivieren

Sicherheitsstandards aktivieren und deaktivieren

Sie können jeden Sicherheitsstandard, der in Security Hub verfügbar ist, aktivieren oder deaktivieren.

Bevor Sie Sicherheitsstandards aktivieren, stellen Sie sicher, dass Sie die Ressourcenaufzeichnung aktiviert AWS Config und konfiguriert haben. Andernfalls ist Security Hub möglicherweise nicht in der Lage, Ergebnisse für die Kontrollen zu generieren, die für einen Standard gelten. Weitere Informationen finden Sie unter Konfiguration AWS Config.

> **Note**
>
> Die Anweisungen zur Aktivierung und Deaktivierung von Standards variieren je nachdem, ob Sie die zentrale Konfiguration verwenden oder nicht. In diesem Abschnitt werden die Unterschiede beschrieben. Die zentrale Konfiguration steht Benutzern zur Verfügung, die

Security Hub und integrieren AWS Organizations. Wir empfehlen, die zentrale Konfiguration zu verwenden, um das Aktivieren und Deaktivieren von Standards in Umgebungen mit mehreren Konten und mehreren Regionen zu vereinfachen.

Aktivierung eines Sicherheitsstandards

Wenn Sie einen Sicherheitsstandard aktivieren, werden alle Steuerelemente, die für den Standard gelten, darin automatisch aktiviert. Security Hub beginnt auch damit, Ergebnisse für Kontrollen zu generieren, die für den Standard gelten.

Sie können in jedem Standard auswählen, welche Steuerelemente aktiviert und deaktiviert werden sollen. Wenn Sie ein Steuerelement deaktivieren, werden keine Ergebnisse für das Steuerelement generiert, und das Steuerelement wird bei der Berechnung der Sicherheitsbewertungen ignoriert.

Wenn Sie Security Hub aktivieren, berechnet Security Hub innerhalb von 30 Minuten nach Ihrem ersten Besuch der Übersichtsseite oder der Seite Sicherheitsstandards in der Security Hub-Konsole die anfängliche Sicherheitsbewertung für einen Standard. In den Regionen China und kann es bis zu 24 Stunden dauern, bis zum ersten Mal Sicherheitsbewertungen generiert werden. AWS GovCloud (US) Region Bewertungen werden nur für Standards generiert, die aktiviert sind, wenn Sie diese Seiten besuchen. Darüber hinaus muss die AWS Config Ressourcenaufzeichnung konfiguriert sein, damit Ergebnisse angezeigt werden. Nach der erstmaligen Generierung des Scores aktualisiert Security Hub den Sicherheits-Score alle 24 Stunden. Security Hub zeigt einen Zeitstempel an, der angibt, wann eine Sicherheitsbewertung zuletzt aktualisiert wurde. Rufen Sie die API auf, um eine Liste der Standards einzusehen, die derzeit in Ihrem Konto aktiviert sind. GetEnabledStandards

Aktivierung eines Standards für mehrere Konten und Regionen

Um einen Sicherheitsstandard für mehrere Konten und zu aktivieren AWS-Regionen, müssen Sie die zentrale Konfiguration verwenden.

Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte Administrator Security Hub Hub-Konfigurationsrichtlinien erstellen, die einen oder mehrere Standards aktivieren. Anschließend können Sie die Konfigurationsrichtlinie bestimmten Konten und Organisationseinheiten (OUs) oder dem Stamm zuordnen. Eine Konfigurationsrichtlinie wird in Ihrer Heimatregion (auch Aggregationsregion genannt) und allen verknüpften Regionen wirksam.

Konfigurationsrichtlinien bieten Anpassungsmöglichkeiten. Sie können beispielsweise festlegen, dass in einer AWS Organisationseinheit nur die Best Practices (Foundation Security Best Practices,

FSBP) und in einer anderen Organisationseinheit FSBP und der Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 aktiviert werden. Anweisungen zum Erstellen einer Konfigurationsrichtlinie, die bestimmte Standards aktiviert, finden Sie unter Security Hub Hub-Konfigurationsrichtlinien erstellen und zuordnen

Wenn Sie die zentrale Konfiguration verwenden, aktiviert Security Hub nicht automatisch Standards in neuen oder bestehenden Konten. Stattdessen definiert der delegierte Administrator bei der Erstellung einer Konfigurationsrichtlinie, welche Standards für verschiedene Konten aktiviert werden sollen. Security Hub bietet eine empfohlene Konfigurationsrichtlinie, in der nur FSBP aktiviert ist. Weitere Informationen finden Sie unter Arten von Konfigurationsrichtlinien.

> **Note**
>
> Der delegierte Administrator kann Konfigurationsrichtlinien erstellen, um jeden Standard außer Service-Managed Standard zu aktivieren:. AWS Control Tower Sie können diesen Standard nur im Service aktivieren. AWS Control Tower Wenn Sie die zentrale Konfiguration verwenden, können Sie die Steuerungen in diesem Standard nur für ein zentral verwaltetes Konto in aktivieren und deaktivieren AWS Control Tower.

Wenn Sie möchten, dass einige Konten ihre eigenen Standards konfigurieren und nicht der delegierte Administrator, kann der delegierte Administrator diese Konten als selbstverwaltet kennzeichnen. Selbstverwaltete Konten müssen die Standards in jeder Region separat konfigurieren.

Aktivierung eines Standards in einem einzigen Konto und einer Region

Wenn Sie keine zentrale Konfiguration verwenden oder wenn Sie ein selbstverwaltetes Konto haben, können Sie keine Konfigurationsrichtlinien verwenden, um Standards in mehreren Konten und Regionen zentral zu aktivieren. Sie können jedoch die folgenden Schritte verwenden, um einen Standard in einem einzigen Konto und einer Region zu aktivieren.

Security Hub console

Um einen Standard in einem Konto und einer Region zu aktivieren

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Vergewissern Sie sich, dass Sie Security Hub in der Region verwenden, in der Sie den Standard aktivieren möchten.

3. Wählen Sie im Security Hub-Navigationsbereich die Option Sicherheitsstandards aus.
4. Wählen Sie für den Standard, den Sie aktivieren möchten, Enable (Aktivieren) aus. Dadurch werden auch alle Kontrollen innerhalb dieses Standards aktiviert.
5. Wiederholen Sie dies in jeder Region, in der Sie den Standard aktivieren möchten.

Security Hub API

Um einen Standard in einem Konto und einer Region zu aktivieren

1. Rufen Sie die BatchEnableStandardsAPI auf.
2. Geben Sie den Amazon-Ressourcennamen (ARN) des Standards an, den Sie aktivieren möchten. Rufen Sie die DescribeStandardsAPI auf, um den Standard-ARN zu erhalten.
3. Wiederholen Sie dies in jeder Region, in der Sie den Standard aktivieren möchten.

AWS CLI

Um einen Standard in einem Konto und einer Region zu aktivieren

1. Führen Sie den Befehl batch-enable-standards aus.
2. Geben Sie den Amazon-Ressourcennamen (ARN) des Standards an, den Sie aktivieren möchten. Führen Sie den describe-standardsBefehl aus, um den Standard-ARN zu erhalten.

```
aws securityhub batch-enable-standards --standards-subscription-requests
 '{"StandardsArn": "standard ARN"}'
```

Beispiel

```
aws securityhub batch-enable-standards --standards-subscription-requests
 '{"StandardsArn":"arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"}'
```

3. Wiederholen Sie dies in jeder Region, in der Sie den Standard aktivieren möchten.

Automatische Aktivierung der Standardsicherheitsstandards

Wenn Sie keine zentrale Konfiguration verwenden, aktiviert Security Hub automatisch Standardsicherheitsstandards für neue Konten, wenn diese Ihrer Organisation beitreten. Alle

Kontrollen, die Teil der Standardstandards sind, werden ebenfalls automatisch aktiviert. Derzeit sind die Standardsicherheitsstandards, die automatisch aktiviert werden, AWS Foundational Security Best Practices (FSBP) und Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Sie können automatisch aktivierte Standards deaktivieren, wenn Sie es vorziehen, Standards in neuen Konten manuell zu aktivieren.

Wenn Sie die zentrale Konfiguration verwenden, können Sie eine Konfigurationsrichtlinie erstellen, die die Standardstandards aktiviert, und diese Richtlinie dem Stammverzeichnis zuordnen. Alle Unternehmenskonten und Organisationseinheiten übernehmen diese Konfigurationsrichtlinie, sofern sie nicht mit einer anderen Richtlinie verknüpft sind oder selbst verwaltet werden.

Schalten Sie automatisch aktivierte Standards aus

Die folgenden Schritte gelten nur, wenn Sie die zentrale Konfiguration integrieren, diese AWS Organizations aber nicht verwenden. Wenn Sie die Organisationsintegration nicht verwenden, können Sie einen Standardstandard deaktivieren, wenn Sie Security Hub zum ersten Mal aktivieren, oder Sie können die Schritte zur Deaktivierung eines Standards befolgen.

Security Hub console

Um automatisch aktivierte Standards auszuschalten

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit den Anmeldeinformationen des Administratorkontos an.
2. Wählen Sie im Security Hub-Navigationsbereich unter Einstellungen die Option Konfiguration aus.
3. Deaktivieren Sie im Abschnitt Konten die Option Standardstandards automatisch aktivieren.

Security Hub API

Um automatisch aktivierte Standards zu deaktivieren

1. Rufen Sie die UpdateOrganizationConfigurationAPI über das Security Hub-Administratorkonto auf.
2. Um automatisch aktivierte Standards in neuen Mitgliedskonten zu deaktivieren, setzen Sie den `AutoEnableStandards` Wert auf`NONE`.

AWS CLI

Um automatisch aktivierte Standards zu deaktivieren

1. Führen Sie den Befehl update-organization-configuration aus.
2. Fügen Sie den `auto-enable-standards` Parameter hinzu, um automatisch aktivierte Standards in neuen Mitgliedskonten zu deaktivieren.

```
aws securityhub update-organization-configuration --auto-enable-standards
```

Einen Sicherheitsstandard deaktivieren

Wenn Sie einen Sicherheitsstandard in Security Hub deaktivieren, passiert Folgendes:

- Alle Kontrollen, die für den Standard gelten, sind ebenfalls deaktiviert, sofern sie nicht mit einem anderen Standard verknüpft sind.
- Prüfungen auf die deaktivierten Steuerelemente werden nicht mehr durchgeführt, und es werden keine weiteren Ergebnisse für die deaktivierten Steuerelemente generiert.
- Bestehende Ergebnisse für deaktivierte Kontrollen werden nach etwa 3—5 Tagen automatisch archiviert.
- Die AWS Config Regeln, die Security Hub für die deaktivierten Steuerelemente erstellt hat, wurden entfernt.

  Dies geschieht normalerweise innerhalb weniger Minuten, nachdem Sie den Standard deaktiviert haben, kann aber länger dauern. Wenn die erste Anfrage zum Löschen der AWS Config Regeln fehlschlägt, versucht Security Hub es alle 12 Stunden erneut. Wenn Sie Security Hub jedoch deaktiviert haben oder keine anderen Standards aktiviert haben, kann Security Hub die Anfrage nicht erneut versuchen, was bedeutet, dass die AWS Config Regeln nicht gelöscht werden können. Wenn dies der Fall ist und Sie AWS Config Regeln löschen müssen, wenden AWS Support Sie sich an.

Deaktivierung eines Standards für mehrere Konten und Regionen

Um einen Sicherheitsstandard für mehrere Konten und Regionen zu deaktivieren, müssen Sie die zentrale Konfiguration verwenden.

Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte Administrator Konfigurationsrichtlinien erstellen, die einen oder mehrere Standards deaktivieren. Sie können eine Konfigurationsrichtlinie bestimmten Konten und Organisationseinheiten oder dem Stamm zuordnen. Eine Konfigurationsrichtlinie wird in Ihrer Heimatregion (auch Aggregationsregion genannt) und allen verknüpften Regionen wirksam.

Konfigurationsrichtlinien bieten Anpassungsmöglichkeiten. Sie können sich beispielsweise dafür entscheiden, den Payment Card Industry Data Security Standard (PCI DSS) in einer Organisationseinheit und sowohl PCI DSS als auch SP 800-53 Rev. 5 des National Institute of Standards and Technology (NIST) in einer anderen Organisationseinheit zu deaktivieren. Anweisungen zum Erstellen einer Konfigurationsrichtlinie, die bestimmte Standards deaktiviert, finden Sie unter. Security Hub Hub-Konfigurationsrichtlinien erstellen und zuordnen

> **Note**
>
> Der delegierte Administrator kann Konfigurationsrichtlinien erstellen, um jeden Standard außer dem Service-Managed Standard zu deaktivieren:. AWS Control Tower Sie können diesen Standard nur im Service deaktivieren. AWS Control Tower Wenn Sie die zentrale Konfiguration verwenden, können Sie die Steuerungen in diesem Standard nur für ein zentral verwaltetes Konto in aktivieren und deaktivieren AWS Control Tower.

Wenn Sie möchten, dass einige Konten ihre eigenen Standards konfigurieren und nicht der delegierte Administrator, kann der delegierte Administrator diese Konten als selbstverwaltet kennzeichnen. Selbstverwaltete Konten müssen die Standards in jeder Region separat konfigurieren.

Deaktivierung eines Standards in einem einzelnen Konto und einer Region

Wenn Sie keine zentrale Konfiguration verwenden oder ein selbstverwaltetes Konto haben, können Sie keine Konfigurationsrichtlinien verwenden, um Standards in mehreren Konten und Regionen zentral zu deaktivieren. Sie können jedoch die folgenden Schritte verwenden, um einen Standard in einem einzelnen Konto und einer Region zu deaktivieren.

Security Hub console

Um einen Standard in einem Konto und einer Region zu deaktivieren

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

2. Vergewissern Sie sich, dass Sie Security Hub in der Region verwenden, in der Sie den Standard deaktivieren möchten.
3. Wählen Sie im Security Hub-Navigationsbereich die Option Sicherheitsstandards aus.
4. Wählen Sie für den Standard, den Sie deaktivieren möchten, Disable (Deaktivieren) aus.
5. Wiederholen Sie dies in jeder Region, in der Sie den Standard deaktivieren möchten.

Security Hub API

Um einen Standard in einem Konto und einer Region zu deaktivieren

1. Rufen Sie die BatchDisableStandardsAPI auf.
2. Geben Sie für jeden Standard, den Sie deaktivieren möchten, den Standard-Abonnement-ARN an. Rufen Sie die API auf, um die Abonnement-ARNs für Ihre aktivierten Standards GetEnabledStandardsabzurufen.
3. Wiederholen Sie dies in jeder Region, in der Sie den Standard deaktivieren möchten.

AWS CLI

Um einen Standard in einem Konto und einer Region zu deaktivieren

1. Führen Sie den Befehl batch-disable-standards aus.
2. Geben Sie für jeden Standard, den Sie deaktivieren möchten, den Standard-Abonnement-ARN an. Führen Sie den get-enabled-standardsBefehl aus, um die Abonnement-ARNs für Ihre aktivierten Standards abzurufen.

```
aws securityhub batch-disable-standards --standards-subscription-arns "standard
 subscription ARN"
```

Beispiel

```
aws securityhub batch-disable-standards --standards-subscription-arns
 "arn:aws:securityhub:us-west-1:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0"
```

3. Wiederholen Sie den Vorgang in jeder Region, in der Sie den Standard deaktivieren möchten.

Details für einen Standard anzeigen

Auf der AWS Security Hub Konsole enthält die Detailseite für einen Standard die folgenden Informationen:

- Die Standardsicherheitsbewertung und eine visuelle Zusammenfassung der Sicherheitsüberprüfungen für die Kontrollen, die im Standard aktiviert sind. Bei der Integration mit gelten Steuerelemente AWS Organizations, die in mindestens einem Organisationskonto aktiviert sind, als aktiviert.
- Die Einstellungen zum Aktivieren oder Deaktivieren eines Steuerelements, das für den Standard gilt.
- Eine Liste von Steuerelementen, die für den Standard gelten. Die Steuerelemente sind je nach Aktivierungsstatus in verschiedene Registerkarten unterteilt. Die Anzahl der Steuerelemente in der Spalte Alle aktiviert entspricht der Summe der Steuerelemente in den Spalten Fehlgeschlagen, Unbekannt, Keine Daten und Bestanden.

Sie können auch die Security Hub Hub-API verwenden und AWS CLI Details für einen Standard abrufen. In den folgenden Abschnitten wird erklärt, wie Sie Details für einen Standard abrufen.

Anzeige der Detailseite für einen aktivierten Standard (Konsole)

Auf der Seite mit den Sicherheitsstandards können Sie die Detailseite für einen aktivierten Standard anzeigen.

Wenn Sie mit dem Administratorkonto angemeldet sind, können Sie Details für jeden Standard anzeigen, der in mindestens einem Mitgliedskonto aktiviert ist.

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Security Hub-Navigationsbereich die Option Sicherheitsstandards aus.
3. Wählen Sie für den Standard, für den Sie die Details anzeigen möchten, die Option Ergebnisse anzeigen aus.

Standard-Sicherheitsbewertung und Zusammenfassung der Sicherheitsüberprüfungen

Oben auf der Seite mit den Standarddetails befindet sich die Sicherheitsbewertung für den Standard. Die Punktzahl ist der Prozentsatz der bestandenen Kontrollen im Verhältnis zur Anzahl der aktivierten Kontrollen (die Daten enthalten) für den Standard.

Security Hub berechnet die anfängliche Sicherheitsbewertung in der Regel innerhalb von 30 Minuten nach Ihrem ersten Besuch der Übersichtsseite oder der Seite Sicherheitsstandards in der Security Hub Hub-Konsole. Bewertungen werden nur für Standards generiert, die aktiviert sind, wenn Sie diese Seiten besuchen. Verwenden Sie den `GetEnabledStandards`API-Vorgang, um eine Liste der derzeit aktivierten Standards anzuzeigen. Darüber hinaus muss die AWS Config Ressourcenaufzeichnung konfiguriert werden, damit die Ergebnisse angezeigt werden. Nach der erstmaligen Generierung des Scores aktualisiert Security Hub den Sicherheits-Score alle 24 Stunden. Security Hub zeigt einen Zeitstempel an, der angibt, wann eine Sicherheitsbewertung zuletzt aktualisiert wurde. Weitere Informationen finden Sie unter the section called “Ermittlung von Sicherheitseinstufungen”.

> **Note**
>
> In den chinesischen Regionen und kann es bis zu 24 Stunden dauern, bis zum ersten Mal Sicherheitsbewertungen generiert werden. AWS GovCloud (US) Region

Neben dem Ergebnis befindet sich ein Diagramm, in dem die Sicherheitsüberprüfungen für Kontrollen zusammengefasst sind, die für den Standard aktiviert sind. Das Diagramm zeigt den Prozentsatz der fehlgeschlagenen und bestandenen Sicherheitsüberprüfungen. Wenn Sie im Diagramm eine Pause einlegen, wird im Pop-up Folgendes angezeigt:

- Die Anzahl der fehlgeschlagenen Sicherheitsüberprüfungen für Kontrollen jedes Schweregrads
- Die Anzahl der Sicherheitsprüfungen für Kontrollen mit dem Status Unbekannt
- Die Anzahl der bestandenen Sicherheitsüberprüfungen

Bei Administratorkonten werden die Standardpunktzahl und das Diagramm für das Administratorkonto und alle Mitgliedskonten zusammengefasst.

Alle Daten auf den Detailseiten zu den Sicherheitsstandards beziehen sich auf die aktuelle Region, sofern Sie keine Aggregationsregion festgelegt haben. Wenn Sie eine Aggregationsregion festgelegt haben, gelten die Sicherheitsbewertungen für alle Regionen und beinhalten Ergebnisse in allen verknüpften Regionen. Der Konformitätsstatus der Kontrollen auf den Seiten mit den Standarddetails spiegelt auch Ergebnisse aus verknüpften Regionen wider, und die Anzahl der Sicherheitsprüfungen umfasst Ergebnisse aus verknüpften Regionen.

Die Kontrollen in aktivierten Standards anzeigen

Wenn Sie die Detailseite für einen Standard aufrufen, können Sie sich eine Liste der Sicherheitskontrollen ansehen, die für den Standard gelten. Diese Liste ist nach dem Konformitätsstatus der Kontrolle und dem Schweregrad sortiert, der jeder Kontrolle zugewiesen wurde. Security Hub aktualisiert den Kontrollstatus und die Anzahl der Sicherheitschecks alle 24 Stunden. Ein Zeitstempel auf jeder Registerkarte gibt an, wann der Kontrollstatus und die Anzahl der Sicherheitschecks zuletzt aktualisiert wurden. Weitere Informationen finden Sie unter the section called “Konformitätsstatus und Kontrollstatus”.

Bei Administratorkonten werden der Status der Kontrollkonformität und die Anzahl der Sicherheitsüberprüfungen für das Administratorkonto und alle Mitgliedskonten zusammengefasst.

Auf der Registerkarte Alle aktiviert sind alle Steuerelemente aufgeführt, die derzeit im Standard aktiviert sind. Bei Administratorkonten enthält die Registerkarte Alle aktiviert Steuerelemente, die standardmäßig in ihrem Konto oder in mindestens einem Mitgliedskonto aktiviert sind.

Auf den Registerkarten Fehlgeschlagen, Unbekannt, Keine Daten und Bestanden werden die Steuerelemente auf der Registerkarte Alle aktiviert so gefiltert, dass sie nur aktivierte Steuerelemente mit einem bestimmten Status enthalten.

Die Registerkarte Deaktiviert enthält die Liste der Steuerelemente, die standardmäßig deaktiviert sind. Für Administratorkonten enthält die Registerkarte Deaktiviert Steuerelemente, die standardmäßig in ihrem Konto und allen Mitgliedskonten deaktiviert sind.

Für jedes Steuerelement werden auf den Registerkarten die folgenden Informationen angezeigt:

- Der Status des Steuerelements (siehethe section called “Konformitätsstatus und Kontrollstatus”)
- Der Schweregrad, der der Kontrolle zugewiesen wurde
- Die Kontroll-ID und der Titel
- Die Anzahl der fehlgeschlagenen aktiven Ergebnisse im Verhältnis zur Gesamtzahl der aktiven Ergebnisse. Falls zutreffend, wird in der Spalte Fehlgeschlagene Prüfungen auch die Anzahl der Ergebnisse mit dem Status Unbekannt aufgeführt.

Zusätzlich zum Suchfilter auf jeder Registerkarte können Sie die Listen nach den folgenden Feldern sortieren:

- Status der Einhaltung der Vorschriften

- Schweregrad
- ID (ID)
- Titel
- Fehlgeschlagene Prüfungen

Sie können jede Liste anhand einer beliebigen Spalte sortieren. Standardmäßig ist die Registerkarte Alle aktiviert so sortiert, dass fehlgeschlagene Steuerelemente ganz oben in der Liste stehen. Auf diese Weise können Sie sich sofort auf Probleme konzentrieren, die behoben werden müssen.

Auf den verbleibenden Registerkarten sind die Steuerelemente standardmäßig in absteigender Reihenfolge nach Schweregrad sortiert. Mit anderen Worten, zuerst werden kritische Kontrollen angezeigt, gefolgt von Kontrollen mit hohem, dann mittlerem und dann niedrigem Schweregrad.

Wählen Sie Ihre bevorzugte Zugriffsmethode und folgen Sie den Schritten, um die verfügbaren Kontrollen für einen aktivierten Standard anzuzeigen. Anstelle dieser Anweisungen können Sie auch den DescribeStandardsControlAPI-Vorgang verwenden.

Security Hub console

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Sicherheitsstandards aus.
3. Wählen Sie Ergebnisse für einen Standard anzeigen aus. Unten auf der Seite werden die Steuerelemente (unterteilt durch Tabs) aufgeführt, die für den Standard gelten.

Security Hub API

1. Führen Sie einen standardmäßigen Amazon-Ressourcennamen (ARN) aus `ListSecurityControlDefinitions`und geben Sie ihn an, um eine Liste der Kontroll-IDs für diesen Standard zu erhalten. Um Standard-ARNs zu erhalten, führen Sie `DescribeStandards`den Befehl aus. Wenn Sie keinen Standard-ARN angeben, gibt diese API alle Security Hub-Steuerungs-IDs zurück. Diese API gibt standardunabhängige Sicherheitskontroll-IDs zurück, keine standardspezifischen Kontroll-IDs.

   Beispiel für eine Anfrage:

   ```
   {
   ```

```
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
best-practices/v/1.0.0"
}
```

2. Führen Sie den Vorgang aus, ListStandardsControlAssociations um herauszufinden, ob in jedem Standard, den Sie in Ihrem Konto aktiviert haben, ein Steuerelement aktiviert ist.
3. Identifizieren Sie das Steuerelement, indem Sie `SecurityControlId` oder angeben`SecurityControlArn`. Paginierungsparameter sind optional.

   Beispiel für eine Anfrage:

```
{
    SecurityControlId: Config.1
    NextToken: lkeyusdlk-sdlflsnd-ladfterb
    MaxResults: 5
}
```

AWS CLI

1. Führen Sie den `list-security-control-definitions` Befehl aus und geben Sie einen oder mehrere Standard-ARNs an, um eine Liste von Kontroll-IDs zu erhalten. Führen Sie den Befehl aus, um Standard-ARNs zu erhalten. `describe-standards` Wenn Sie keinen Standard-ARN angeben, gibt dieser Befehl alle Security Hub-Steuerungs-IDs zurück. Dieser Befehl gibt standardunabhängige Sicherheitskontroll-IDs zurück, keine standardspezifischen Kontroll-IDs.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Führen Sie den `list-standards-control-associations` Befehl aus, um herauszufinden, ob in jedem Standard, den Sie in Ihrem Konto aktiviert haben, ein Steuerelement aktiviert ist.
3. Identifizieren Sie das Steuerelement, indem Sie `security-control-id` oder angeben`security-control-arn`.

   Beispielbefehl:

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id Config.1
```

Die Liste der Steuerelemente wird heruntergeladen

Sie können die aktuelle Seite der Kontrollliste in eine `.csv` Datei herunterladen.

Wenn Sie die Steuerelementliste gefiltert haben, enthält die heruntergeladene Datei nur die Steuerelemente, die den Filtereinstellungen entsprechen.

Wenn Sie ein bestimmtes Steuerelement aus der Liste ausgewählt haben, enthält die heruntergeladene Datei nur dieses Steuerelement.

Um die aktuelle Seite der Steuerelementliste oder das aktuell ausgewählte Steuerelement herunterzuladen, wählen Sie Herunterladen.

Steuerungen in bestimmten Standards aktivieren und deaktivieren

Wenn Sie einen Standard in aktivieren AWS Security Hub, werden alle Steuerelemente, die für ihn gelten, automatisch in diesem Standard aktiviert (die Ausnahme bilden servicemanagierte Standards). Anschließend können Sie bestimmte Steuerelemente im Standard deaktivieren und wieder aktivieren. Wir empfehlen jedoch, den Aktivierungsstatus eines Steuerelements auf alle aktivierten Standards abzustimmen.

> **Note**
>
> Wenn Sie die zentrale Konfiguration von Security Hub verwenden, kann der delegierte Administrator Kontrollen für Organisationskonten für alle aktivierten Standards aktivieren und deaktivieren. Wir empfehlen diesen Ansatz, damit der Aktivierungsstatus einer Steuerung standardübergreifend einheitlich ist. Der delegierte Administrator kann jedoch Konten als selbstverwaltete Konten kennzeichnen, sodass er Kontrollen in bestimmten Standards aktivieren und deaktivieren kann. Weitere Informationen finden Sie unter So funktioniert die zentrale Konfiguration.

Die Detailseite für einen Standard enthält die Liste der für den Standard geltenden Kontrollen sowie Informationen darüber, welche Kontrollen derzeit in diesem Standard aktiviert und deaktiviert sind.

Auf der Seite mit den Standarddetails können Sie auch Steuerelemente in einem bestimmten Standard aktivieren und deaktivieren. Sie müssen die Steuerelemente in beiden Bereichen separat aktivieren AWS-Konto und deaktivieren AWS-Region. Wenn Sie ein Steuerelement aktivieren oder deaktivieren, wirkt sich dies nur auf das aktuelle Konto und die Region aus.

Sie können Steuerungen in jeder Region mithilfe der Security Hub-Konsole, der Security Hub-API oder aktivieren und deaktivieren AWS CLI. Wenn Sie eine Aggregationsregion festgelegt haben, werden Ihnen Steuerungen aus allen verknüpften Regionen angezeigt. Wenn ein Steuerelement in einer verknüpften Region verfügbar ist, aber nicht in der Aggregationsregion, können Sie dieses Steuerelement nicht in der Aggregationsregion aktivieren oder deaktivieren. Skripts zur Deaktivierung von Steuerungen für mehrere Konten und Regionen finden Sie unter Security Hub-Steuerelemente in einer Umgebung mit mehreren Konten deaktivieren.

Ein Steuerelement in einem bestimmten Standard aktivieren

Um ein Steuerelement in einem Standard zu aktivieren, müssen Sie zunächst mindestens einen Standard aktivieren, für den das Steuerelement gilt. Weitere Hinweise zur Aktivierung eines Standards finden Sie unterSicherheitsstandards aktivieren und deaktivieren. Wenn Sie ein Steuerelement in einem Standard aktivieren, AWS Security Hub beginnt die Generierung von Ergebnissen für dieses Steuerelement. Security Hub bezieht den Kontrollstatus in die Berechnung der Gesamtsicherheitsbewertung und der Standardsicherheitsbewertungen ein. Selbst wenn Sie eine Kontrolle in mehreren Standards aktivieren, erhalten Sie bei jeder standardübergreifenden Sicherheitsüberprüfung nur ein Ergebnis, wenn Sie die konsolidierten Kontrollergebnisse aktivieren. Weitere Informationen finden Sie unter Konsolidierte Erkenntnisse zu Kontrollen.

Um eine Kontrolle in einem Standard zu aktivieren, muss die Kontrolle in Ihrer aktuellen Region verfügbar sein. Weitere Informationen finden Sie unter Verfügbarkeit von Steuerelementen nach Regionen.

Gehen Sie wie folgt vor, um ein Security Hub-Steuerelement in einem bestimmten Standard zu aktivieren. Anstelle der folgenden Schritte können Sie auch die `UpdateStandardsControl`API-Aktion verwenden, um Kontrollen in einem bestimmten Standard zu aktivieren. Anweisungen zur Aktivierung eines Steuerelements in allen Standards finden Sie unterAktivierung einer Steuerung nach allen Standards in einem einzigen Konto und einer einzigen Region.

Security Hub console

So aktivieren Sie ein Steuerelement in einem bestimmten Standard

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich die Option Sicherheitsstandards aus.
3. Wählen Sie Ergebnisse anzeigen für den entsprechenden Standard aus.
4. Wählen Sie ein Steuerelement aus.
5. Wählen Sie Steuerung aktivieren (diese Option wird nicht für ein Steuerelement angezeigt, das bereits aktiviert ist). Bestätigen Sie, indem Sie „Aktivieren“ wählen.

Security Hub API

Um ein Steuerelement in einem bestimmten Standard zu aktivieren

1. Führen Sie `ListSecurityControlDefinitions` einen Standard-ARN aus und geben Sie ihn an, um eine Liste der verfügbaren Steuerelemente für einen bestimmten Standard abzurufen. Führen Sie den Befehl aus, um einen Standard-ARN zu erhalten `DescribeStandards`. Diese API gibt standardunabhängige Sicherheitskontroll-IDs zurück, keine standardspezifischen Kontroll-IDs.

   Beispiel für eine Anfrage:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Führen Sie `ListStandardsControlAssociations` den Vorgang aus und geben Sie eine spezifische Kontroll-ID an, um den aktuellen Aktivierungsstatus eines Steuerelements in jedem Standard zurückzugeben.

   Beispiel für eine Anfrage:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. Führen Sie BatchUpdateStandardsControlAssociations. Geben Sie den ARN des Standards an, in dem Sie das Steuerelement aktivieren möchten.
4. Stellen Sie den `AssociationStatus` Parameter auf`ENABLED`.

   Beispiel für eine Anfrage:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}]
}
```

AWS CLI

Um ein Steuerelement in einem bestimmten Standard zu aktivieren

1. Führen Sie den list-security-control-definitions Befehl aus und geben Sie einen Standard-ARN an, um eine Liste der verfügbaren Steuerelemente für einen bestimmten Standard abzurufen. Führen Sie den Befehl aus, um einen Standard-ARN zu erhaltendescribe-standards. Dieser Befehl gibt standardunabhängige Sicherheitskontroll-IDs zurück, keine standardspezifischen Kontroll-IDs.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Führen Sie den list-standards-control-associations Befehl aus und geben Sie eine spezifische Kontroll-ID an, um den aktuellen Aktivierungsstatus eines Steuerelements in jedem Standard zurückzugeben.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Führen Sie den Befehl batch-update-standards-control-associations aus. Geben Sie den ARN des Standards an, in dem Sie das Steuerelement aktivieren möchten.
4. Stellen Sie den `AssociationStatus` Parameter auf`ENABLED`.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
```

```
 "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
```

Deaktivierung eines Steuerelements in einem bestimmten Standard

Wenn Sie ein Steuerelement in einem Standard deaktivieren, generiert Security Hub keine Ergebnisse mehr für das Steuerelement. Der Kontrollstatus wird bei der Berechnung der Sicherheitsbewertung für den Standard nicht mehr verwendet.

Eine Möglichkeit, ein Steuerelement zu deaktivieren, besteht darin, alle Standards zu deaktivieren, für die das Steuerelement gilt. Wenn Sie einen Standard deaktivieren, werden alle Steuerelemente, die für den Standard gelten, deaktiviert (diese Steuerelemente können jedoch in anderen Standards weiterhin aktiviert bleiben). Hinweise zur Deaktivierung eines Standards finden Sie unterthe section called “Aktivieren und Deaktivieren von Standards”.

Wenn Sie ein Steuerelement deaktivieren, indem Sie einen Standard deaktivieren, für den es gilt, passiert Folgendes:

- Sicherheitsüberprüfungen für das Steuerelement werden für diesen Standard nicht mehr durchgeführt. Das bedeutet, dass der Kontrollstatus keinen Einfluss auf die Standardsicherheitsbewertung hat (Security Hub führt weiterhin Sicherheitsprüfungen für das Steuerelement durch, wenn es in anderen Standards aktiviert ist).
- Für dieses Steuerelement werden keine zusätzlichen Funde generiert.
- Bestehende Ergebnisse werden automatisch nach 3—5 Tagen archiviert (beachten Sie, dass dies nach bestem Wissen erfolgt und nicht garantiert werden kann).
- Die zugehörigen AWS Config Regeln, die Security Hub erstellt hat, wurden entfernt.

Wenn Sie einen Standard deaktivieren, verfolgt Security Hub nicht, welche Steuerelemente deaktiviert wurden. Wenn Sie den Standard anschließend wieder aktivieren, werden alle Steuerelemente, die für ihn gelten, automatisch aktiviert. Darüber hinaus ist das Deaktivieren eines Steuerelements eine einmalige Aktion. Angenommen, Sie deaktivieren ein Steuerelement und aktivieren dann einen Standard, der zuvor deaktiviert war. Wenn der Standard dieses Steuerelement enthält, wird es in diesem Standard aktiviert. Wenn Sie einen Standard in Security Hub aktivieren, werden alle Kontrollen, die für diesen Standard gelten, automatisch aktiviert.

Anstatt ein Steuerelement zu deaktivieren, indem Sie einen Standard deaktivieren, für den es gilt, können Sie das Steuerelement einfach in einem oder mehreren bestimmten Standards deaktivieren.

Um das Suchgeräusch zu reduzieren, kann es nützlich sein, Steuerungen zu deaktivieren, die für Ihre Umgebung nicht relevant sind. Empfehlungen dazu, welche Steuerelemente Sie deaktivieren sollten, finden Sie unter Security Hub-Steuerelemente, die Sie möglicherweise deaktivieren möchten.

Gehen Sie wie folgt vor, um ein Steuerelement in bestimmten Standards zu deaktivieren. Anstelle der folgenden Schritte können Sie auch die `UpdateStandardsControl`API-Aktion verwenden, um Steuerelemente in einem bestimmten Standard zu deaktivieren. Anweisungen zum Deaktivieren eines Steuerelements in allen Standards finden Sie unterAktivierung und Deaktivierung von Steuerungen in allen Standards.

Security Hub console

So deaktivieren Sie ein Steuerelement in einem bestimmten Standard

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich die Option Sicherheitsstandards aus. Wählen Sie Ergebnisse anzeigen für den entsprechenden Standard aus.
3. Wählen Sie ein Steuerelement aus.
4. Wählen Sie Steuerung deaktivieren (diese Option wird nicht für ein Steuerelement angezeigt, das bereits deaktiviert ist).
5. Geben Sie einen Grund für die Deaktivierung des Steuerelements an und bestätigen Sie, indem Sie „Deaktivieren“ wählen.

Security Hub API

Um ein Steuerelement in einem bestimmten Standard zu deaktivieren

1. Führen Sie `ListSecurityControlDefinitions` einen Standard-ARN aus und geben Sie ihn an, um eine Liste der verfügbaren Steuerelemente für einen bestimmten Standard abzurufen. Führen Sie den Befehl aus, um einen Standard-ARN zu erhalten `DescribeStandards`. Diese API gibt standardunabhängige Sicherheitskontroll-IDs zurück, keine standardspezifischen Kontroll-IDs.

   Beispiel für eine Anfrage:

```
{
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
best-practices/v/1.0.0"
}
```

2. Führen Sie ListStandardsControlAssociations den Vorgang aus und geben Sie eine spezifische Kontroll-ID an, um den aktuellen Aktivierungsstatus eines Steuerelements in jedem Standard zurückzugeben.

   Beispiel für eine Anfrage:

```
{
    "SecurityControlId": "IAM.1"
}
```

3. Führen Sie BatchUpdateStandardsControlAssociations. Geben Sie den ARN des Standards an, in dem Sie das Steuerelement deaktivieren möchten.
4. Stellen Sie den `AssociationStatus` Parameter auf`DISABLED`. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits deaktiviert ist, gibt die API eine Antwort mit dem HTTP-Statuscode 200 zurück.

   Beispiel für eine Anfrage:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED",  "UpdatedReason": "Not applicable to
 environment"}]
}
```

AWS CLI

Um ein Steuerelement in einem bestimmten Standard zu deaktivieren

1. Führen Sie den list-security-control-definitions Befehl aus und geben Sie einen Standard-ARN an, um eine Liste der verfügbaren Steuerelemente für einen bestimmten Standard abzurufen. Führen Sie den Befehl aus, um einen Standard-ARN zu erhaltendescribe-standards. Dieser Befehl gibt standardunabhängige Sicherheitskontroll-IDs zurück, keine standardspezifischen Kontroll-IDs.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Führen Sie den list-standards-control-associations Befehl aus und geben Sie eine spezifische Kontroll-ID an, um den aktuellen Aktivierungsstatus eines Steuerelements in jedem Standard zurückzugeben.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Führen Sie den Befehl batch-update-standards-control-associations aus. Geben Sie den ARN des Standards an, in dem Sie das Steuerelement deaktivieren möchten.
4. Stellen Sie den `AssociationStatus` Parameter auf`DISABLED`. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits aktiviert ist, gibt der Befehl eine Antwort mit dem HTTP-Statuscode 200 zurück.

```
aws securityhub  --region us-east-1 batch-update-standards-control-
associations --standards-control-association-updates '[{"SecurityControlId":
 "CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED",
 "UpdatedReason": "Not applicable to environment"}]'
```

Referenz zu Security Hub-Steuerungen

Diese Kontrollreferenz enthält eine Liste der verfügbaren AWS Security Hub Steuerelemente mit Links zu weiteren Informationen zu den einzelnen Steuerelementen. In der Übersichtstabelle werden die Steuerelemente in alphabetischer Reihenfolge nach der Kontroll-ID angezeigt. Nur Steuerelemente, die von Security Hub aktiv verwendet werden, sind hier enthalten. Nicht mehr verwendete Steuerelemente sind von dieser Liste ausgenommen. Die Tabelle enthält die folgenden Informationen für jedes Steuerelement:

- ID der Sicherheitskontrolle — Diese ID gilt für alle Standards und gibt die AWS-Service Ressource an, auf die sich die Kontrolle bezieht. In der Security Hub Hub-Konsole werden Sicherheitskontroll-IDs angezeigt, unabhängig davon, ob die konsolidierten Kontrollergebnisse in Ihrem Konto aktiviert oder deaktiviert sind. Security Hub Hub-Ergebnisse verweisen jedoch nur dann auf

Sicherheitskontroll-IDs, wenn konsolidierte Kontrollergebnisse in Ihrem Konto aktiviert sind. Wenn konsolidierte Kontrollbefunde in Ihrem Konto deaktiviert sind, variieren einige Kontroll-IDs je nach Standard in Ihren Kontrollergebnissen. Eine Zuordnung von standardspezifischen Kontroll-IDs zu Sicherheitskontroll-IDs finden Sie unter. Wie sich die Konsolidierung auf Kontroll-IDs und Titel auswirkt

Wenn Sie Automatisierungen für Sicherheitskontrollen einrichten möchten, empfehlen wir, anhand der Kontroll-ID und nicht anhand des Titels oder der Beschreibung zu filtern. Security Hub kann zwar gelegentlich Titel oder Beschreibungen von Kontrollen aktualisieren, die Kontroll-IDs bleiben jedoch gleich.

Bei Kontroll-IDs können Zahlen übersprungen werden. Dies sind Platzhalter für future Kontrollen.

- Anwendbare Standards — Gibt an, für welche Standards eine Kontrolle gilt. Wählen Sie eine Kontrolle aus, um sich spezifische Anforderungen von Compliance-Frameworks von Drittanbietern anzusehen.
- Titel Sicherheitskontrolle — Dieser Titel gilt für alle Standards. In der Security Hub Hub-Konsole werden Titel der Sicherheitskontrollen angezeigt, unabhängig davon, ob die konsolidierten Kontrollergebnisse in Ihrem Konto aktiviert oder deaktiviert sind. Security Hub Hub-Ergebnisse verweisen jedoch nur dann auf Titel der Sicherheitskontrolle, wenn konsolidierte Kontrollergebnisse in Ihrem Konto aktiviert sind. Wenn die Option „Konsolidierte Kontrollbefunde“ in Ihrem Konto deaktiviert ist, variieren einige Kontrolltitel je nach Standard in Ihren Kontrollergebnissen. Eine Zuordnung von standardspezifischen Kontroll-IDs zu Sicherheitskontroll-IDs finden Sie unter. Wie sich die Konsolidierung auf Kontroll-IDs und Titel auswirkt
- Schweregrad — Der Schweregrad einer Kontrolle gibt an, wie wichtig sie aus Sicherheitsgründen ist. Informationen darüber, wie Security Hub den Schweregrad der Kontrolle bestimmt, finden Sie unterDen Kontrollergebnissen den Schweregrad zuweisen.
- Zeitplantyp — Gibt an, wann die Kontrolle bewertet wird. Weitere Informationen finden Sie unter Zeitplan für die Ausführung von Sicherheitsprüfungen.
- Unterstützt benutzerdefinierte Parameter — Gibt an, ob das Steuerelement benutzerdefinierte Werte für einen oder mehrere Parameter unterstützt. Wählen Sie ein Steuerelement aus, um die Parameterdetails anzuzeigen. Weitere Informationen finden Sie unter Benutzerdefinierte Steuerungsparameter.

Wählen Sie ein Steuerelement aus, um weitere Details anzuzeigen. Die Steuerelemente werden in alphabetischer Reihenfolge des Dienstnamens aufgeführt.

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Account.1	Sicherheitskontaktinformationen sollten für eine bereitgestellt werden AWS-Konto	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
Konto.2	AWS-Konto sollte Teil einer Organisation sein AWS Organizations	NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Regelmäßig
ACM.1	Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst und periodisch
ACM.2	Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ACM.3	ACM-Zertifikate sollten gekennzeichnet sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
APIGateway.1	API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst
APIGateway.2	API Gateway, REST-API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
APIGateway.3	Bei den REST-API-Stufen von API Gateway sollte die AWS X-Ray Ablaufverfolgung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
APIGateway.4	API Gateway sollte mit einer WAF-Web-ACL verknüpft sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
APIGateway.5	API-Gateway-REST-API-Cache-Daten sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
APIGateway.8	API-Gateway-Routen sollten einen Autorisierungstyp angeben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
APIGateway.9	Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
AppSync2.2	AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	 Ja	Änderung ausgelöst
AppSync4.	AWS AppSync GraphQL-APIs sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
AppSync5.	AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
Athena.2	Athena-Datenkataloge sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
Athena.3	Athena-Arbeitsgruppen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
AutoScaling1.	Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
AutoScaling2.	Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst
AutoScaling3.	Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
AutoScaling.5	Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
AutoScaling6.	Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden.	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
AutoScaling9.	EC2 Auto Scaling Scaling-Gruppen sollten EC2-Startvorlagen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
AutoScaling1.0	EC2 Auto Scaling Scaling-Gruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Sicherung.1	AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Sicherung.2	AWS Backup Wiederherstellungspunkte sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
Sicherung.3	AWS Backup Tresore sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
Sicherung.4	AWS Backup Berichtspläne sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
Sicherung.4	AWS Backup Backup-Pläne sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
CloudFormation2.	CloudFormation Stapel sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudFront.1.	CloudFront Bei Distributionen sollte ein Standard-Root-Objekt konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
CloudFront.3.	CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
CloudFront.4.	CloudFront Bei Distributionen sollte Origin Failover konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
CloudFront.5.	CloudFront Bei Distributionen sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
CloudFront.6.	CloudFront Bei Distributionen sollte WAF aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudFront7.	CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
CloudFront8.	CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
CloudFront9.	CloudFront Distributionen sollten den Verkehr zu benutzerdefinierten Ursprüngen verschlüsseln	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
CloudFront10	CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudFront.2	CloudFront Verteilungen sollten nicht auf nicht existierende S3-Ursprünge verweisen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Regelmäßig
CloudFront.3	CloudFront Distributionen sollten Origin Access Control verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	MITTEL	 Nein	Änderung ausgelöst
CloudFront.4	CloudFront Distributionen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
CloudTrail.1	CloudTrail sollte mit mindestens einem multiregionalen Trail aktiviert und konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst	CIS AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (HOCH)	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudTrail.2	CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert sein	CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
CloudTrail.3	Mindestens ein CloudTrail Trail sollte aktiviert sein	PCI DSS v3.2.1	HIGH (HOCH)	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudTrail4.	CloudTrail Die Überprüfung der Protokolldatei sollte aktiviert sein	CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Regelmäßig
CloudTrail5.	CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden	CIS AWS Foundations Benchmark v1.2.0, Best Practices für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudTrail6.	Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist	Benchmark AWS für GUS-Stiftungen v1.2.0, Benchmark für AWS GUS-Stiftungen v1.4.0	KRITISCH	 Nein	Änderung ausgelöst und periodisch
CloudTrail7.	Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist	Benchmark AWS für GUS-Stiftungen v1.2.0, Benchmark für AWS GUS-Stiftungen v1.4.0	NIEDRIG	 Nein	Regelmäßig
CloudTrail9.	CloudTrail Wege sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
CloudWatch1.	Für die Verwendung des Root-Benutzers sollten ein Log-Metrikfilter und ein Alarm vorhanden sein	CIS AWS Foundations Benchmark v1.2.0, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS	NIEDRIG	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudWatch.2.	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind	Benchmark AWS v1.2.0 für CIS Foundations	NIEDRIG	 Nein	Regelmäßig
CloudWatch.3.	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung in der Managementkonsole ohne MFA vorhanden sind	Benchmark AWS v1.2.0 für CIS Foundations	NIEDRIG	 Nein	Regelmäßig
CloudWatch.4	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der IAM-Richtlinie vorhanden sind	Benchmark für AWS GUS-Stiftungen v1.2.0, Benchmark für AWS GIS-Stiftungen v1.4.0	NIEDRIG	 Nein	Regelmäßig
CloudWatch.5.	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind	Benchmark AWS für GUS-Stiftungen v1.2.0, Benchmark für AWS GUS-Stiftungen v1.4.0	NIEDRIG	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudWatch6.	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind	Benchmark AWS für GUS-Stiftungen v1.2.0, Benchmark für AWS GUS-Stiftungen v1.4.0	NIEDRIG	 Nein	Regelmäßig
CloudWatch7.	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden erstellten CMKs vorhanden sind	Benchmark für AWS GUS-Stiftungen v1.2.0, Benchmark für AWS GUS-Stiftungen v1.4.0	NIEDRIG	 Nein	Regelmäßig
CloudWatch8.	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind	Benchmark für AWS GUS-Stiftungen v1.2.0, Benchmark für AWS GUS-Stiftungen v1.4.0	NIEDRIG	 Nein	Regelmäßig
CloudWatch9.	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Config Konfigurationsänderungen vorhanden sind	Benchmark AWS für GUS-Stiftungen v1.2.0, Benchmark für AWS GUS-Stiftungen v1.4.0	NIEDRIG	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudWatch.10	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Sicherheitsgruppe vorhanden sind	Benchmark für AWS GUS-Stiftungen v1.2.0, Benchmark für AWS GUS-Stiftungen v1.4.0	NIEDRIG	 Nein	Regelmäßig
CloudWatch.11	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind	Benchmark für AWS GUS-Stiftungen v1.2.0, Benchmark für AWS GUS-Stiftungen v1.4.0	NIEDRIG	 Nein	Regelmäßig
CloudWatch1.2	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an Network-Gateways vorhanden sind	Benchmark für AWS GUS-Stiftungen v1.2.0, Benchmark für AWS GUS-Stiftungen v1.4.0	NIEDRIG	 Nein	Regelmäßig
CloudWatch1.3	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Routing-Tabelle vorhanden sind	Benchmark für AWS GUS-Stiftungen v1.2.0, Benchmark für AWS GUS-Stiftungen v1.4.0	NIEDRIG	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CloudWatch.14	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für VPC-Änderungen vorhanden sind	Benchmark für AWS GUS-Stiftungen v1.2.0, Benchmark für AWS GUS-Stiftungen v1.4.0	NIEDRIG	 Nein	Regelmäßig
CloudWatch1,5	CloudWatch Für Alarme sollten bestimmte Aktionen konfiguriert sein	NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Ja	Änderung ausgelöst
CloudWatch1.6	CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden	NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
CloudWatch1,7	CloudWatch Alarmaktionen sollten aktiviert sein	NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
CodeArtifact1.	CodeArtifact Repositorien sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CodeBuild 1.	CodeBuild Die URLs des Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst
CodeBuild 2.	CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS AWS Control Tower v3.2.1, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst
CodeBuild 3.	CodeBuild S3-Protokolle sollten verschlüsselt sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
CodeBuild 4.	CodeBuild Projektumgebungen sollten über eine Protokollierungskonfiguration verfügen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Config.1	AWS Config sollte aktiviert sein	CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, PCI DSS v3.2.1, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
DataFirehose1.	Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
Detektiv. 1	Verhaltensdiagramme von Detektiven sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DMS.1	Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard:, PCI DSS AWS Control Tower v3.2.1, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Regelmäßig
DMS.2	DMS-Zertifikate sollten mit einem Tag versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
DMS.3	DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
DMS.4	DMS-Replikationsinstanzen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
DMS.5	Subnetzgruppen für die DMS-Replikation sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DMS.6	Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
DMS.7	Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
DMS.8	Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
DMS.9	DMS-Endpunkte sollten SSL verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
DMS.10	Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DMS.11	Auf DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
DMS.12	Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
DocumentDB DB.1	Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
DocumentDB DB.2	Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	MITTEL	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DocumentDB DB.3	Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst
DocumentDB DB.4	Amazon DocumentDB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
DocumentDB DB.5	Für Amazon DocumentDB-Cluster sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
DynamoDB 1	DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DynamoDB 2	DynamoDB DynamoDB-Tabellen sollte die Wiederherstellung aktiviert point-in-time sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
DynamoDB 3	DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
DynamoDB.4	DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein	NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
DynamoDB.5	DynamoDB-Tabellen sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
DynamoDB,6	DynamoDB DynamoDB-Tabellen sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
DynamoDB.7	DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
EC2.1	EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Regelmäßig
EC2.2	VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen	CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.3	Angehängte EBS-Volumes sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
EC2.4	Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
EC2.6	Die VPC-Flussprotokollierung sollte in allen VPCs aktiviert sein	CIS AWS Foundations Benchmark v1.2.0, Best Practices für AWS grundlegende Sicherheit v1.0.0, Service Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, CIS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5 AWS	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.7	Die EBS-Standardverschlüsselung sollte aktiviert sein	AWS Bewährte Methoden für grundlegende Sicherheit v1.0.0, Service Managed Standard:, CIS AWS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
EC2.8	EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (HOCH)	 Nein	Änderung ausgelöst
EC2.9	EC2-Instances sollten keine öffentliche IPv4-Adresse haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.10	Amazon EC2 sollte so konfiguriert sein, dass VPC-Endpunkte verwendet werden, die für den Amazon EC2-Service erstellt wurden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MITTEL	 Nein	Regelmäßig
EC2.12	Ungenutzte EC2-EIPs sollten entfernt werden	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
EC2.13	Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen	Benchmark für CIS AWS Foundations v1.2.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
EC2,14	Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen	AWS Benchmark v1.2.0 für CIS Foundations	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.15	EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
EC2.16	Unbenutzte Network Access Control Lists sollten entfernt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
EC2.17	EC2-Instances sollten nicht mehrere ENIs verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.18	Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Verkehr für autorisierte Ports zulassen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Ja	Änderung ausgelöst
EC2.19	Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst
EC2.20	Beide VPN-Tunnel für eine AWS Site-to-Site-VPN-Verbindung sollten aktiv sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.21	Netzwerk-ACLs sollten keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, CIS Foundations Benchmark v1.4.0, NIST SP 800-53 AWS Control Tower Rev. 5 AWS	MITTEL	 Nein	Änderung ausgelöst
EC2.22	Ungenutzte EC2-Sicherheitsgruppen sollten entfernt werden	Vom Service verwalteter Standard: AWS Control Tower	MITTEL	 Nein	Regelmäßig
EC2.23	EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
EC2.24	Paravirtuelle EC2-Instance-Typen sollten nicht verwendet werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.25	EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
EC2.28	EBS-Volumes sollten in einem Backup-Plan enthalten sein	NIST SP 800-53 Rev. 5	NIEDRIG	 Ja	Regelmäßig
EC 2,33	EC2-Transit-Gateway-Anhänge sollten gekennzeichnet werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
EC2.34	Die Routentabellen des EC2-Transit-Gateways sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
EC2.35	EC2-Netzwerkschnittstellen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.36	EC2-Kunden-Gateways sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
EC2.37	Elastische EC2-IP-Adressen sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
EC2.38	EC2-Instances sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
EC2.39	EC2-Internet-Gateways sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
EC2.40	EC2-NAT-Gateways sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
EC2.41	EC2-Netzwerk-ACLs sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
EC2.42	EC2-Routing-Tabellen sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
EC2.43	EC2-Sicherheitsgruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.44	EC2-Subnetze sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
EC2.45	EC2-Volumes sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
EC2.46	Amazon VPCs sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
EC2.47	Amazon VPC Endpoint Services sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
EC2.48	Amazon VPC-Flow-Logs sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
EC2.49	Amazon VPC-Peering-Verbindungen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
EC2.50	EC2-VPN-Gateways sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EC2.51	Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
EC2.52	EC2-Transit-Gateways sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
EC2.53	EC2-Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 auf Remote-Serveradministrationsports zulassen	AWS Benchmark v3.0.0 für CIS Foundations	HIGH (HOCH)	 Nein	Regelmäßig
EC 2.54	EC2-Sicherheitsgruppen sollten keinen Zugriff von: :/0 zu Remote-Serververwaltungsports zulassen	Benchmark v3.0.0 für CIS Foundations AWS	HIGH (HOCH)	 Nein	Regelmäßig
ECR.1	In privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ECR.2	Für private ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
ECR.3	Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ECR.4	Öffentliche ECR-Repositorien sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
ECS.1	Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ECS.2	ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
ECS.3	ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
ECS.4	ECS-Container sollten ohne Zugriffsrechte ausgeführt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ECS.5	ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (HOCH)	 Nein	Änderung ausgelöst
ECS.8	Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
ECS.9	ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
ECS.10	Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion ausgeführt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ECS.12	ECS-Cluster sollten Container Insights verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ECS.13	ECS-Dienste sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
ECS.14	ECS-Cluster sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
ECS.15	ECS-Aufgabendefinitionen sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
EFS.1	Elastic File System sollte so konfiguriert sein, dass es Dateidaten im Ruhezustand verschlüsselt AWS KMS	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EFS.2	Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
EFS.3	EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
EFS.4	EFS-Zugriffspunkte sollten eine Benutzeridentität erzwingen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
EFS. 5	EFS-Zugangspunkte sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EFS. 6	EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Nein	Regelmäßig
EKS.1	EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Regelmäßig
EKS.2	EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
EKS.3	EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
EKS. 6	EKS-Cluster sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EKS.7	Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
EKS.8	Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
ElastiCache1.	ElastiCache Bei Redis-Clustern sollte die automatische Sicherung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Ja	Regelmäßig
ElastiCache2.2	ElastiCache für Redis-Cache-Cluster sollten auto Nebenversions-Upgrades aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Regelmäßig
ElastiCache3.	ElastiCache Für Replikationsgruppen sollte automatisches Failover aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ElastiCache4.	ElastiCache Replikationsgruppen hätten aktiviert sein müssen encryption-at-rest	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
ElastiCache5.	ElastiCache Replikationsgruppen sollten aktiviert sein encryption-in-transit	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
ElastiCache6.	ElastiCache Für Replikationsgruppen früherer Redis-Versionen sollte Redis AUTH aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
ElastiCache7.	ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ElasticBeanstalk1.	In Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
ElasticBeanstalk2.	Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Ja	Änderung ausgelöst
ElasticBeanstalk3.	Elastic Beanstalk sollte Logs streamen nach CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0	HIGH (HOCH)	 Ja	Änderung ausgelöst
ELB.1	Der Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden.	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ELB.2	Classic Load Balancer mit SSL/HTTPS-Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
ELB.3	Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden.	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ELB.4	Der Application Load Balancer sollte so konfiguriert sein, dass er HTTP-Header löscht	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ELB.5	Die Protokollierung von Anwendungen und Classic Load Balancers sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ELB.6	Für Anwendung, Gateway und Network Load Balancer sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ELB.7	Bei Classic Load Balancers sollte der Verbindungsabbau aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ELB.8	Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Konfiguration verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ELB.9	Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ELB.10	Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ELB.12	Der Application Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
ELB.13	Load Balancer für Anwendungen, Netzwerke und Gateways sollten sich über mehrere Availability Zones erstrecken	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst
ELB.14	Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
ELB.16	Application Load Balancer sollten mit einer Web-ACL verknüpft sein AWS WAF	NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
EMR.1	Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Regelmäßig
EMR. 2	Die Einstellung „Öffentlichen Zugriff blockieren“ in Amazon EMR sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Regelmäßig
ES.1	Für Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ES.2	Elasticsearch-Domains sollten nicht öffentlich zugänglich sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Regelmäßig
ES.3	Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ES.4	Die Protokollierung von Elasticsearch-Domänenfehlern in CloudWatch Logs sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ES.5	Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ES.6	Elasticsearch-Domains sollten mindestens drei Datenknoten haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ES.7	Elasticsearch-Domains sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ES.8	Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
ES.9	Elasticsearch-Domains sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
EventBridge2.	EventBridge Eventbusse sollten gekennzeichnet sein	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
EventBridge3.	EventBridge maßgeschneiderte Eventbusse sollten mit einer ressourcenbasierten Richtlinie versehen sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
EventBridge4.	EventBridge Auf globalen Endpunkten sollte die Ereignisreplikation aktiviert sein	NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
FSX. 1	FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden.	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
FSX. 2	FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
Kleber.1	AWS Glue Jobs sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
GlobalAccelerator1.	Global Accelerator-Beschleuniger sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
GuardDuty 1.	GuardDuty sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS AWS Control Tower v3.2.1, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
GuardDuty 2.2.	GuardDuty Filter sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
GuardDuty 3.	GuardDuty IPSets sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
GuardDuty 4.	GuardDuty Detektoren sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
IAM.1	IAM-Richtlinien sollten keine vollen „*“ - Administratorrechte zulassen	CIS AWS Foundations Benchmark v1.2.0, Best Practices für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.2	IAM-Benutzern sollten keine IAM-Richtlinien zugewiesen sein	CIS AWS Foundations Benchmark v1.2.0, Best Practices für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
IAM.3	Die Zugangsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden	CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard:, CIS AWS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.4	Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren	CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Regelmäßig
IAM.5	MFA sollte für alle IAM-Benutzer aktiviert sein, die ein Konsolenpasswort haben	CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard:, CIS AWS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.6	Hardware-MFA sollte für den Root-Benutzer aktiviert sein	CIS AWS Foundations Benchmark v1.2.0, Bewährte Methoden für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Regelmäßig
IAM.7	Passwortrichtlinien für IAM-Benutzer sollten starke Konfigurationen haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.8	Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden	CIS AWS Foundations Benchmark v1.2.0, Best Practices für AWS grundlegende Sicherheit v1.0.0, Service-Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
IAM.9	MFA sollte für den Root-Benutzer aktiviert sein	CIS AWS Foundations Benchmark v1.2.0, PCI DSS v3.2.1, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Regelmäßig
ICH BIN .10	Die Kennwortrichtlinien für IAM-Benutzer sollten solide Konfigurationen haben	PCI DSS v3.2.1	MITTEL	 Nein	Regelmäßig
IAM.11	Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert	Benchmark v1.2.0 der CIS AWS Foundations	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.12	Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert	Benchmark v1.2.0 der CIS AWS Foundations	MITTEL	 Nein	Regelmäßig
IAM.13	Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist	Benchmark v1.2.0 der CIS AWS Foundations	MITTEL	 Nein	Regelmäßig
IAM.14	Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert	Benchmark v1.2.0 der CIS AWS Foundations	MITTEL	 Nein	Regelmäßig
IAM.15	Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert	CIS AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0	MITTEL	 Nein	Regelmäßig
IAM.16	Sicherstellen, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert	Benchmark AWS für GUS-Stiftungen v1.2.0, Benchmark für AWS GUS-Stiftungen v1.4.0	NIEDRIG	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.17	Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft	Benchmark v1.2.0 der CIS AWS Foundations	NIEDRIG	 Nein	Regelmäßig
IAM.18	Stellen Sie sicher, dass eine Support-Rolle für die Bearbeitung von Vorfällen eingerichtet wurde mit AWS Support	Benchmark AWS für GUS-Stiftungen v1.2.0, Benchmark für AWS GUS-Stiftungen v1.4.0	NIEDRIG	 Nein	Regelmäßig
ICH BIN. 19	MFA sollte für alle IAM-Benutzer aktiviert sein	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
IAM.21	Von Ihnen erstellte, vom Kunden verwaltete IAM-Richtlinien sollten keine Platzhalteraktionen für Dienste zulassen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IAM.22	IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden	Benchmark v1.4.0 der CIS AWS Foundations	MITTEL	 Nein	Regelmäßig
ICH BIN.23	IAM Access Analyzer-Analyzer sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
ICH BIN.24	IAM-Rollen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
ICH BIN .25	IAM-Benutzer sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	 Ja	Änderung ausgelöst
ICH BIN .26	Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden	Benchmark v3.0.0 für CIS Foundations AWS	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
ICH BIN. 27	IAM-Identitäten sollte die Richtlinie nicht beigefügt sein AWSCloudShellFullAccess	Benchmark v3.0.0 für CIS AWS Foundations	MITTEL	 Nein	Änderung ausgelöst
ICH BIN .28	Der externe Zugriffsanalysator von IAM Access Analyzer sollte aktiviert sein	Benchmark AWS v3.0.0 für CIS Foundations	HIGH (HOCH)	 Nein	Regelmäßig
IoT. 1	AWS IoT Core Sicherheitsprofile sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
IoT.2	AWS IoT Core Maßnahmen zur Schadensbegrenzung sollten gekennzeichnet werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
IoT.3	AWS IoT Core Abmessungen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
IoT.4	AWS IoT Core Autorisierer sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
IoT.5	AWS IoT Core Rollenaliase sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
IoT. 6	AWS IoT Core Richtlinien sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
Kinesis.1	Kinesis-Streams sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Kinese.2	Kinesis-Streams sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
KMS.1	Vom Kunden verwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
KMS.2	IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
KMS.3	AWS KMS keys sollte nicht ungewollt gelöscht werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst
KMS.4	AWS KMS key Rotation sollte aktiviert sein	CIS AWS Foundations Benchmark v1.2.0, PCI DSS v3.2.1, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Lambda.1	Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst
Lambda.2	Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Lambda.3	Lambda-Funktionen sollten sich in einer VPC befinden	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
Lambda.5	VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Lambda.6	Lambda-Funktionen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
Macie.1	Amazon Macie sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
Macie.2	Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Regelmäßig
MSK.1	MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
MSK.2	Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein	NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
MQ. 2	ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
MQ. 3	Amazon MQ-Broker sollten das automatische Upgrade der Nebenversion aktiviert haben	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
MQ. 4	Amazon MQ-Broker sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
MQ.5	ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden	NIST SP 800-53 Rev. 5, durch Service verwalteter Standard: AWS Control Tower	NIEDRIG	 Nein	Änderung ausgelöst
MQ.6	RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden	NIST SP 800-53 Rev. 5, vom Service verwalteter Standard: AWS Control Tower	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Neptun.1	Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
Neptun.2	Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
Neptun.3	Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	KRITISCH	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Neptun.4	Neptune Neptune-DB-Clustern sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	NIEDRIG	 Nein	Änderung ausgelöst
Neptun.5	Neptune Neptune-DB-Clustern sollten automatische Backups aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	MITTEL	 Ja	Änderung ausgelöst
Neptun.6	Neptune DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Neptun.7	Neptune Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed-Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
Neptun.8	Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	NIEDRIG	 Nein	Änderung ausgelöst
Neptun.9	Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden	NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
NetworkFirewall1.	Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden	NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
NetworkFirewall2.	Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
NetworkFirewall3.	Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
NetworkFirewall4.	Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ lauten.	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
NetworkFirewall5.	Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ lauten.	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
NetworkFirewall6.	Die Regelgruppe der Stateless Network Firewall sollte nicht leer sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
NetworkFirewall7.	Netzwerk-Firewall-Firewalls sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
NetworkFirewall8.	Netzwerk-Firewall-Firewall-Richtlinien sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
NetworkFirewall9.	Network Firewall Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
OpenSearch.1	OpenSearch Bei Domänen sollte die Verschlüsselung im Ruhezustand aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS AWS Control Tower v3.2.1, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
OpenSearch.2	OpenSearch Domains sollten nicht öffentlich zugänglich sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS AWS Control Tower v3.2.1, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
OpenSearch.3	OpenSearch Domänen sollten Daten verschlüsseln, die zwischen Knoten gesendet werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
OpenSearch.4	OpenSearch Die Protokollierung von Domänenfehlern in CloudWatch Logs sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
OpenSearch.5	OpenSearch Für Domänen sollte die Auditprotokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
OpenSearch.6	OpenSearch Domänen sollten mindestens drei Datenknoten haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
OpenSearch.7	OpenSearch Für Domänen sollte eine fein abgestufte Zugriffskontrolle aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
OpenSearch.8	Verbindungen zu OpenSearch Domänen sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Suche öffnen.9	OpenSearch Domains sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Suche öffnen.10	OpenSearch Auf den Domains sollte das neueste Softwareupdate installiert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
Opensearch.11	OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben	NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
PCA.1	AWS Private CA Die Stammzertifizierungsstelle sollte deaktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Regelmäßig
RDS.1	Der RDS-Snapshot sollte privat sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS AWS Control Tower v3.2.1, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.2	RDS-DB-Instances sollten, wie in der Konfiguration festgelegt, den PubliclyAccessible öffentlichen Zugriff verbieten	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst
RDS.3	Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service Managed Standard:, CIS AWS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
RDS.4	RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.5	RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
RDS.6	Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Ja	Änderung ausgelöst
RDS.7	Bei RDS-Clustern sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.8	Für RDS-DB-Instances sollte der Löschschutz aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
RDS.9	RDS-DB-Instances sollten CloudWatch Protokolle in Logs veröffentlichen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
RDS.10	Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.11	Für RDS-Instances sollten automatische Backups aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst
RDS.12	Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
RDS.13	Automatische RDS-Upgrades für kleinere Versionen sollten aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
RDS.14	Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.15	RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
RDS.16	RDS-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
RDS.17	RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
RDS.18	RDS-Instances sollten in einer VPC bereitgestellt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.19	Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Clusterereignisse konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
RDS.20	Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
RDS.21	Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.22	Für kritische Ereignisse in Datenbank sicherheitsgruppen sollte ein Abonnement für RDS-Ereignisbenachrichtigungen konfiguriert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
RDS.23	RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
RDS.24	RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.25	RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
RDS.26	RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden	NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
RDS.27	RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5, Service-Managed Standard: AWS Control Tower	MITTEL	 Nein	Änderung ausgelöst
RDS.28	RDS-DB-Cluster sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
RDS.29	Snapshots des RDS-DB-Clusters sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
RDS.30	RDS-DB-Instances sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
RDS.31	RDS-DB-Sicherheitsgruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
RDS.32	RDS-DB-Snapshots sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
RDS.33	RDS-DB-Subnetzgruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
RDS.34	Aurora MySQL-DB-Cluster sollten Audit-Logs in CloudWatch Logs veröffentlichen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
RDS.35	Für RDS-DB-Cluster sollte das automatische Upgrade der Nebenversionen aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Redshift.1	Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst
Redshift.2	Verbindungen zu Amazon Redshift Redshift-Clustern sollten während der Übertragung verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Redshift.3	Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Redshift.4	Amazon Redshift Redshift-Cluster sollte die Audit-Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Redshift.6	Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Redshift.7	Redshift-Cluster sollten erweitertes VPC-Routing verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Redshift.8	Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Redshift.9	Redshift-Cluster sollten nicht den Standarddatenbanknamen verwenden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Redshift.10	Redshift-Cluster sollten im Ruhezustand verschlüsselt werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
Rotverschiebung.11	Redshift-Cluster sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
Rotverschiebung.12	Abonnementbenachrichtigungen für Redshift-Ereignisse sollten mit Tags versehen werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
Rotverschiebung.13	Redshift-Cluster-Snapshots sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
Rotverschiebung.14	Redshift-Cluster-Subnetzgruppen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst
Rotverschiebung.15	Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Ursprüngen zulassen	AWS Bewährte grundlegende Sicherheitsmethoden	HIGH (HOCH)	 Nein	Regelmäßig
Route 53.1	Route 53-Gesundheitschecks sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
Route 53.2	In öffentlich gehostete n Zonen von Route 53 sollten DNS-Abfragen protokolliert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
S3.1	Für S3-Allzweck-Buckets sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein	AWS Bewährte Methoden für grundlegende Sicherheit, Service Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
S3.2	S3-Buckets für allgemeine Zwecke sollten den öffentlichen Lesezugriff blockieren	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst und periodisch
S3.3	S3-Buckets für allgemeine Zwecke sollten den öffentlichen Schreibzugriff blockieren	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst und periodisch

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
S3.5	Für S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erforderlich sein	AWS Bewährte Methoden für grundlegende Sicherheit, Service Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
S3.6	Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
S3.7	S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
S3.8	S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren	AWS Bewährte grundlegende Sicherheitsverfahren, Service-Managed-Standard:, CIS AWS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
S3.9	Für S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
S3.10	S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben	NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
S3.11	Für S3-Buckets für allgemeine Zwecke sollten Ereignisbenachrichtigungen aktiviert sein	NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
S3.12	ACLs sollten nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
S3.13	S3-Buckets für allgemeine Zwecke sollten Lifecycle-Konfigurationen haben	AWS Bewährte grundlegende Sicherheitsmethoden, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Ja	Änderung ausgelöst
S3.14	Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein	NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
S3.15	Bei S3-Allzweck-Buckets sollte Object Lock aktiviert sein	NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
S3.17	S3-Buckets für allgemeine Zwecke sollten im Ruhezustand mit verschlüsselt werden AWS KMS keys	Servicemanagierter Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
S3.19	Bei S3-Zugangspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Änderung ausgelöst
S3.20	Für S3-Allzweck-Buckets sollte MFA Delete aktiviert sein	Benchmark v1.4.0 der CIS AWS Foundations, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst
S3.22	S3-Buckets für allgemeine Zwecke sollten Schreiberignisse auf Objektebene protokollieren	Benchmark v3.0.0 für CIS Foundations AWS	MITTEL	 Nein	Regelmäßig
S3.23	S3-Buckets für allgemeine Zwecke sollten Leseereignisse auf Objektebene protokollieren	Benchmark v3.0.0 für CIS Foundations AWS	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SageMaker 1.	Amazon SageMaker Notebook-Instances sollten keinen direkten Internetzugang haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS AWS Control Tower v3.2.1, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Regelmäßig
SageMaker 2.2.	SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
SageMaker 3.	Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instanzen haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SageMaker 4.	SageMaker Bei Produktionsvarianten für Endgeräte sollte die anfängliche Anzahl der Instanzen größer als 1 sein	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
SecretsManager1.	Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Änderung ausgelöst
SecretsManager2.	Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SecretsManager3.	Unbenutzte Secrets Manager Manager-Geheimnisse entfernen	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
SecretsManager4.	Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Ja	Regelmäßig
SecretsManager5.	Secrets Manager Manager-Geheimnisse sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
ServiceCatalog1.	Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SES.1	SES-Kontaktlisten sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
SES.2	SES-Konfigurationssätze sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
SNS.1	SNS-Themen sollten im Ruhezustand verschlüsselt werden mit AWS KMS	NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
SNS.3	SNS-Themen sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
SQS.1	Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
SQS.2	SQS-Warteschlangen sollten markiert werden	AWS Standard für Ressourcen-Tagging	NIEDRIG	Ja	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SSM.1	EC2-Instances sollten verwaltet werden von AWS Systems Manager	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
SSM.2	Von Systems Manager verwaltete EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (HOCH)	 Nein	Änderung ausgelöst
SSM.3	Von Systems Manager verwaltete EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
SSM.4	SSM-Dokumente sollten nicht öffentlich sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	KRITISCH	 Nein	Regelmäßig
StepFunctions1.	Step Functions, bei Zustandsmaschinen sollte die Protokollierung aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden	MITTEL	 Ja	Änderung ausgelöst
StepFunctions2.	Step Functions Functions-Aktivitäten sollten markiert werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
Übertragung.1	Die Workflows von Transfer Family sollten mit Tags versehen werden	AWS Standard für die Kennzeichnung von Ressourcen	NIEDRIG	Ja	Änderung ausgelöst
Übertragung.2	Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden	AWS Bewährte grundlegende Sicherheitsmethoden, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
WAF.1	AWS WAF Die klassische globale Web-ACL-Protokollierung sollte aktiviert sein	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Regelmäßig
WAF.2	AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung enthalten	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
WAF.3	AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
WAF.4	AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed-Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
WAF.6	AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
WAF.7	AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
WAF.8	AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

ID der Sicherheitskontrolle	Titel der Sicherheitskontrolle	Anwendbare Normen	Schweregrad	Unterstützt benutzerdefinierte Parameter	Art des Zeitplans
WAF.10	AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, Service-Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst
WAF.11	AWS WAF Die Web-ACL-Protokollierung sollte aktiviert sein	NIST SP 800-53 Rev. 5	NIEDRIG	 Nein	Regelmäßig
WAF. 12	AWS WAF Für Regeln sollten Metriken aktiviert sein CloudWatch	AWS Bewährte grundlegende Sicherheitsmethoden v1.0.0, NIST SP 800-53 Rev. 5	MITTEL	 Nein	Änderung ausgelöst

Themen

- AWS-Konto steuert
- AWS Certificate Manager Steuerungen
- Amazon API Gateway Gateway-Steuerelemente
- AWS AppSync Steuerungen
- Amazon Athena Athena-Steuerung
- AWS Backup Steuerungen
- AWS CloudFormation steuert
- CloudFront Amazon-Kontrollen

- AWS CloudTrail Steuerungen
- CloudWatch Amazon-Kontrollen
- AWS CodeArtifact Steuerungen
- AWS CodeBuild Steuerungen
- AWS Config steuert
- Amazon Data Firehose-Steuerelemente
- Amazon Detective steuert
- AWS Database Migration Service Steuerungen
- Amazon DocumentDB-Steuerelemente
- Amazon DynamoDB-Steuerelemente
- Kontrollen in der Amazon Elastic Container Registry
- Amazon ECS-Steuerelemente
- Amazon Elastic Compute Cloud-Steuerelemente
- Amazon EC2 Auto Scaling-Steuerelemente
- Amazon EC2 Systems Manager Manager-Steuerelemente
- Steuerelemente für das Amazon Elastic File System
- Steuerelemente für Amazon Elastic Kubernetes Service
- ElastiCache Amazon-Kontrollen
- AWS Elastic Beanstalk steuert
- Elastic Load Balancing Balancing-Steuerelemente
- Amazon EMR-Steuerelemente
- Elasticsearch-Steuerelemente
- EventBridge Amazon-Kontrollen
- Amazon FSx-Steuerelemente
- AWS Global Accelerator steuert
- AWS Glue Steuerungen
- GuardDuty Amazon-Kontrollen
- AWS Identity and Access Management steuert
- AWS IoT steuert

- Amazon Kinesis Kinesis-Steuerung
- AWS Key Management Service steuert
- AWS Lambda steuert
- Amazon Macie-Steuerelemente
- Amazon MSK-Steuerungen
- Amazon MQ-Steuerelemente
- Amazon Neptune Neptune-Steuerungen
- AWS Network Firewall steuert
- Amazon OpenSearch Service-Kontrollen
- AWS Private Certificate Authority steuert
- Steuerelemente von Amazon Relational Database Service
- Amazon Redshift Redshift-Steuerelemente
- Amazon Route 53-Steuerelemente
- Steuerelemente von Amazon Simple Storage Service
- SageMaker Amazon-Kontrollen
- AWS Secrets Manager Steuerungen
- AWS Service Catalog Steuerungen
- Steuerelemente von Amazon Simple Email Service
- Steuerelemente von Amazon Simple Notification Service
- Steuerelemente von Amazon Simple Queue Service
- AWS Step Functions Kontrollen
- AWS Transfer Family Steuerungen
- AWS WAF steuert

AWS-Konto steuert

Diese Kontrollen beziehen sich auf AWS-Konten.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Account.1] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto

Verwandte Anforderungen: NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `security-account-information-provided`

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon Web Services (AWS) -Konto Sicherheitskontaktinformationen enthält. Die Kontrolle schlägt fehl, wenn keine Sicherheitskontaktinformationen für das Konto bereitgestellt werden.

Alternative Sicherheitskontakte AWS ermöglichen es, eine andere Person bei Problemen mit Ihrem Konto zu kontaktieren, falls Sie nicht verfügbar sind. Benachrichtigungen können von AWS Support oder anderen AWS-Service Teams zu sicherheitsrelevanten Themen im Zusammenhang mit Ihrer AWS-Konto Nutzung stammen.

Abhilfe

Informationen zum Hinzufügen eines alternativen Kontakts als Sicherheitskontakt zu Ihrem AWS-Konto finden Sie unter Hinzufügen, Ändern oder Entfernen alternativer Kontakte im AWS Billing and Cost Management-Benutzerhandbuch.

[Account.2] AWS-Konten sollte Teil einer Organisation sein AWS Organizations

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Schweregrad: Hoch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `account-part-of-organizations`

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob ein Teil einer Organisation AWS-Konto ist, die über verwaltet wird AWS Organizations. Die Kontrolle schlägt fehl, wenn das Konto nicht Teil einer Organisation ist.

Organizations hilft Ihnen dabei, Ihre Umgebung zentral zu verwalten, während Sie Ihre Workloads skalieren. AWS Sie können mehrere verwenden AWS-Konten , um Workloads zu isolieren, für die bestimmte Sicherheitsanforderungen gelten, oder um Frameworks wie HIPAA oder PCI einzuhalten. Durch die Gründung einer Organisation können Sie mehrere Konten als eine einzige Einheit verwalten und deren Zugriff AWS-Services, Ressourcen und Regionen zentral verwalten.

Abhilfe

Informationen zum Erstellen einer neuen Organisation und AWS-Konten zum automatischen Hinzufügen finden Sie unter Organisation erstellen im AWS Organizations Benutzerhandbuch. Informationen zum Hinzufügen von Konten zu einer bestehenden Organisation finden Sie im AWS Organizations Benutzerhandbuch unter Einladen einer AWS-Konto Person, Ihrer Organisation beizutreten.

AWS Certificate Manager Steuerungen

Diese Kontrollen beziehen sich auf ACM-Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[ACM.1] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden

Verwandte Anforderungen: NIST.800-53.R5 SC-28 (3), NIST.800-53.R5 SC-7 (16)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten währen der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ACM::Certificate`

AWS Config -Regel: `acm-certificate-expiration-check`

Art des Zeitplans: Ausgelöste und periodische Änderung

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`daysToExpiration`	Anzahl der Tage, innerhalb derer das ACM-Zertifikat erneuert werden muss	Ganzzahl	`14` auf `365`	`30`

Diese Kontrolle prüft, ob ein AWS Certificate Manager (ACM-) Zertifikat innerhalb des angegebenen Zeitraums erneuert wird. Es überprüft sowohl importierte Zertifikate als auch von ACM bereitgestellte Zertifikate. Die Kontrolle schlägt fehl, wenn das Zertifikat nicht innerhalb des angegebenen Zeitraums erneuert wird. Sofern Sie keinen benutzerdefinierten Parameterwert für den Verlängerungszeitraum angeben, verwendet Security Hub einen Standardwert von 30 Tagen.

ACM kann Zertifikate, die DNS-Validierung verwenden, automatisch verlängern. Bei Zertifikaten, die E-Mail-Validierung verwenden, müssen Sie auf eine E-Mail zur Domainvalidierung antworten. ACM erneuert Zertifikate, die Sie importieren, nicht automatisch. Sie müssen importierte Zertifikate manuell erneuern.

Abhilfe

ACM bietet eine verwaltete Verlängerung für Ihre von Amazon ausgestellten SSL/TLS-Zertifikate. Das bedeutet, dass ACM Ihre Zertifikate entweder automatisch erneuert (wenn Sie die DNS-Validierung verwenden) oder Ihnen E-Mail-Benachrichtigungen sendet, wenn der Ablauf des Zertifikats näher rückt. Diese Dienste werden sowohl für öffentliche als auch für private ACM-Zertifikate bereitgestellt.

Für Domains, die per E-Mail validiert wurden

> Wenn ein Zertifikat 45 Tage vor Ablauf abläuft, sendet ACM für jeden Domainnamen eine E-Mail an den Domaininhaber. Um die Domains zu validieren und die Verlängerung abzuschließen, müssen Sie auf die E-Mail-Benachrichtigungen antworten.
>
> Weitere Informationen finden Sie im AWS Certificate Manager Benutzerhandbuch unter Verlängerung für per E-Mail validierte Domains.

Für Domains, die durch DNS validiert wurden

ACM erneuert automatisch Zertifikate, die DNS-Validierung verwenden. 60 Tage vor Ablauf überprüft ACM, ob das Zertifikat erneuert werden kann.

Wenn ein Domainname nicht validiert werden kann, sendet ACM eine Benachrichtigung, dass eine manuelle Validierung erforderlich ist. Diese Benachrichtigungen werden 45 Tage, 30 Tage, 7 Tage und 1 Tag vor Ablauf gesendet.

Weitere Informationen finden Sie im AWS Certificate Manager Benutzerhandbuch unter Verlängerung für durch DNS validierte Domains.

[ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden

Kategorie: Identifizieren > Inventar > Inventarservices

Schweregrad: Hoch

Art der Ressource: `AWS::ACM::Certificate`

AWS Config -Regel: `acm-certificate-rsa-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob RSA-Zertifikate, die mit verwaltet werden, eine Schlüssellänge von mindestens 2.048 Bit AWS Certificate Manager verwenden. Die Steuerung schlägt fehl, wenn die Schlüssellänge kleiner als 2.048 Bit ist.

Die Stärke der Verschlüsselung korreliert direkt mit der Schlüsselgröße. Wir empfehlen Schlüssellängen von mindestens 2.048 Bit, um Ihre AWS Ressourcen zu schützen, da Rechenleistung immer günstiger wird und Server immer fortschrittlicher werden.

Abhilfe

Die Mindestschlüssellänge für von ACM ausgestellte RSA-Zertifikate beträgt bereits 2.048 Bit. Anweisungen zur Ausstellung neuer RSA-Zertifikate mit ACM finden Sie unter Ausstellen und Verwalten von Zertifikaten im Benutzerhandbuch.AWS Certificate Manager

Mit ACM können Sie zwar Zertifikate mit kürzeren Schlüssellängen importieren, Sie müssen jedoch Schlüssel mit mindestens 2.048 Bit verwenden, um diese Kontrolle zu bestehen. Sie können die Schlüssellänge nach dem Import eines Zertifikats nicht ändern. Stattdessen müssen Sie Zertifikate mit einer Schlüssellänge von weniger als 2.048 Bit löschen. Weitere Informationen zum Importieren von Zertifikaten in ACM finden Sie unter Voraussetzungen für den Import von Zertifikaten im AWS Certificate Manager Benutzerhandbuch.

[ACM.3] ACM-Zertifikate sollten mit einem Tag versehen werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::ACM::Certificate`

AWS Config Regel: `tagged-acm-certificate` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Certificate Manager (ACM-) Zertifikat Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Kontrolle schlägt fehl, wenn das Zertifikat keine Tagschlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt

fehl, wenn das Zertifikat mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem ACM-Zertifikat finden Sie unter Kennzeichnen von AWS Certificate Manager Zertifikaten im Benutzerhandbuch.AWS Certificate Manager

Amazon API Gateway Gateway-Steuerelemente

Diese Steuerelemente beziehen sich auf API Gateway Gateway-Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[ApiGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein

Verwandte Anforderungen: NIst.800-53.R5 AC-4 (26), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIst.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp:`AWS::ApiGateway::Stage`, `AWS::ApiGatewayV2::Stage`

AWS Config -Regel: `api-gw-execution-logging-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`loggingLevel`	Protokollierungsstufe	Enum	`ERROR`, `INFO`	`No default value`

Dieses Steuerelement prüft, ob in allen Phasen einer Amazon API Gateway Gateway-REST- oder WebSocket API-Phase die Protokollierung aktiviert ist. Die Kontrolle schlägt fehl, wenn sie `loggingLevel` nicht `ERROR` oder `INFO` für alle Stufen der API gilt. Sofern Sie keine benutzerdefinierten Parameterwerte angeben, um anzugeben, dass ein bestimmter Protokolltyp aktiviert werden soll, erzeugt Security Hub eine erfolgreiche Feststellung, wenn die Protokollierungsebene entweder `ERROR` oder ist`INFO`.

Für API Gateway REST- oder WebSocket API-Stufen sollten die entsprechenden Protokolle aktiviert sein. Die REST- und WebSocket API-Ausführungsprotokollierung von API Gateway bietet detaillierte Aufzeichnungen der Anfragen an die REST- und WebSocket API-Stufen von API Gateway. Die Phasen umfassen Backend-Antworten zur API-Integration, Antworten des Lambda-Autorisierers und die `requestId` For-Integrationsendpunkte. AWS

Abhilfe

Informationen zum Aktivieren der Protokollierung für REST- und WebSocket API-Operationen finden Sie unter CloudWatch API-Protokollierung mithilfe der API-Gateway-Konsole einrichten im API Gateway Developer Guide.

[ApiGateway.2] API Gateway REST-API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden

Verwandte Anforderungen: NIST.800-53.R5 AC-17 (2), NIST.800-53.R5 AC-4, NIST.800-53.R5 IA-5 (1), NIst.800-53.R5 SC-12 (3), NIst.800-53.R5 SC-13, NIst.800-53.R5 SC-23, NIst.800-53.R5 SC-23 (3), NIst.NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategorie: Schützen > Datenschutz

Schweregrad: Mittel

Art der Ressource: `AWS::ApiGateway::Stage`

AWS Config -Regel: `api-gw-ssl-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für die REST-API-Stufen von Amazon API Gateway SSL-Zertifikate konfiguriert sind. Backend-Systeme verwenden diese Zertifikate, um zu authentifizieren, dass eingehende Anfragen von API Gateway stammen.

API Gateway REST API-Stufen sollten mit SSL-Zertifikaten konfiguriert werden, damit Backend-Systeme authentifizieren können, dass Anfragen von API Gateway stammen.

Abhilfe

Detaillierte Anweisungen zum Generieren und Konfigurieren von API Gateway REST API-SSL-Zertifikaten finden Sie unter Generieren und Konfigurieren eines SSL-Zertifikats für die Backend-Authentifizierung im API Gateway Developer Guide.

[ApiGateway.3] Bei den REST-API-Stufen von API Gateway sollte die Ablaufverfolgung aktiviert sein AWS X-Ray

Verwandte Anforderungen: NIST.800-53.r5 CA-7

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Art der Ressource: `AWS::ApiGateway::Stage`

AWS Config -Regel: `api-gw-xray-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob AWS X-Ray Active Tracing für Ihre Amazon API Gateway Gateway-REST-API-Stufen aktiviert ist.

Active Tracing mit X-Ray ermöglicht eine schnellere Reaktion auf Leistungsänderungen in der zugrunde liegenden Infrastruktur. Leistungsänderungen können zu einer mangelnden Verfügbarkeit der API führen. X-Ray Active Tracing bietet Echtzeit-Metriken zu Benutzeranfragen, die über Ihre API-Gateway-REST-API-Operationen und verbundenen Dienste fließen.

Abhilfe

Ausführliche Anweisungen zur Aktivierung von X-Ray Active Tracing für API Gateway REST-API-Operationen finden Sie unter Amazon API Gateway Active Tracing Support for AWS X-Ray im AWS X-Ray Developer Guide.

[ApiGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein

Verwandte Anforderungen: NIST.800-53.R5 AC-4 (21)

Kategorie: Schützen > Schutzdienste

Schweregrad: Mittel

Art der Ressource: `AWS::ApiGateway::Stage`

AWS Config -Regel: `api-gw-associated-with-waf`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein API-Gateway-Schritt eine AWS WAF Web Access Control List (ACL) verwendet. Dieses Steuerelement schlägt fehl, wenn keine AWS WAF Web-ACL an eine REST-API-Gateway-Stufe angehängt ist.

AWS WAF ist eine Firewall für Webanwendungen, die hilft, Webanwendungen und APIs vor Angriffen zu schützen. Damit können Sie eine ACL konfigurieren. Dabei handelt es sich um eine Reihe von Regeln, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre API-Gateway-Stufe mit einer AWS WAF Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Abhilfe

Informationen dazu, wie Sie die API Gateway-Konsole verwenden, um eine AWS WAF regionale Web-ACL einer vorhandenen API-Gateway-API-Stufe zuzuordnen, finden Sie unter Using AWS WAF to protect your APIs im API Gateway Developer Guide.

[ApiGateway.5] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6))

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::ApiGateway::Stage`

AWS Config Regel: `api-gw-cache-encrypted` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob alle Methoden in API Gateway Gateway-REST-API-Stufen, für die der Cache aktiviert ist, verschlüsselt sind. Die Steuerung schlägt fehl, wenn eine Methode in einer API-Gateway-REST-API-Stufe für den Cache konfiguriert ist und der Cache nicht verschlüsselt ist. Security Hub bewertet die Verschlüsselung einer bestimmten Methode nur, wenn das Caching für diese Methode aktiviert ist.

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass auf Daten, die auf der Festplatte gespeichert sind, von einem Benutzer zugegriffen wird, für den kein Benutzer authentifiziert ist. AWS Es fügt weitere Zugriffskontrollen hinzu, um den Zugriff unberechtigter

Benutzer auf die Daten einzuschränken. Beispielsweise sind API-Berechtigungen erforderlich, um die Daten zu entschlüsseln, bevor sie gelesen werden können.

API-Gateway-REST-API-Caches sollten im Ruhezustand verschlüsselt werden, um eine zusätzliche Sicherheitsebene zu gewährleisten.

Abhilfe

Informationen zur Konfiguration von API-Caching für eine Phase finden Sie unter Amazon API Gateway Gateway-Caching aktivieren im API Gateway Developer Guide. Wählen Sie in den Cache-Einstellungen die Option Cache-Daten verschlüsseln aus.

[ApiGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben

Verwandte Anforderungen: NIST.800-53.R5 AC-3, NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Schützen > Sicheres Zugriffsmanagement

Schweregrad: Mittel

Art der Ressource: `AWS::ApiGatewayV2::Route`

AWS Config Regel: `api-gwv2-authorization-type-configured`

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`authorizationType`	Autorisierungstyp der API-Routen	Enum	`AWS_IAM`, `CUSTOM`, `JWT`	Kein Standardwert

Diese Kontrolle prüft, ob Amazon API Gateway Gateway-Routen einen Autorisierungstyp haben. Die Steuerung schlägt fehl, wenn die API-Gateway-Route keinen Autorisierungstyp hat. Optional können Sie einen benutzerdefinierten Parameterwert angeben, wenn das Steuerelement nur dann

übergeben werden soll, wenn die Route den im `authorizationType` Parameter angegebenen Autorisierungstyp verwendet.

API Gateway unterstützt mehrere Mechanismen zur Steuerung und Verwaltung des Zugriffs auf Ihre API. Durch die Angabe eines Autorisierungstyps können Sie den Zugriff auf Ihre API auf autorisierte Benutzer oder Prozesse beschränken.

Abhilfe

Informationen zum Festlegen eines Autorisierungstyps für HTTP-APIs finden Sie unter Steuern und Verwalten des Zugriffs auf eine HTTP-API in API Gateway im API Gateway Developer Guide. Informationen zum Festlegen eines Autorisierungstyps für WebSocket APIs finden Sie unter Steuern und Verwalten des Zugriffs auf eine WebSocket API in API Gateway im API Gateway Developer Guide.

[ApiGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein

Verwandte Anforderungen: NIst.800-53.R5 AC-4 (26), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIst.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::ApiGatewayV2::Stage`

AWS Config Regel: `api-gwv2-access-logs-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung konfiguriert haben. Diese Kontrolle schlägt fehl, wenn die Einstellungen für das Zugriffsprotokoll nicht definiert sind.

API Gateway Gateway-Zugriffsprotokolle enthalten detaillierte Informationen darüber, wer auf Ihre API zugegriffen hat und wie der Anrufer auf die API zugegriffen hat. Diese Protokolle sind für Anwendungen wie Sicherheits- und Zugriffsprüfungen sowie forensische Untersuchungen nützlich. Aktivieren Sie diese Zugriffsprotokolle, um Verkehrsmuster zu analysieren und Probleme zu beheben.

Weitere bewährte Methoden finden Sie unter Monitoring REST APIs im API Gateway Developer Guide.

Abhilfe

Informationen zum Einrichten der Zugriffsprotokollierung finden Sie unter CloudWatch API-Protokollierung mithilfe der API-Gateway-Konsole einrichten im API Gateway Developer Guide.

AWS AppSync Steuerungen

Diese Kontrollen beziehen sich auf AWS AppSync Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp: `AWS::AppSync::GraphQLApi`

AWS Config -Regel: `appsync-logging-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert	
`fieldLoggingLevel`	Ebene der Feldprotokollierung	Enum	`ERROR`, `ALL`	No `default value`	

Dieses Steuerelement prüft, ob für eine AWS AppSync API die Protokollierung auf Feldebene aktiviert ist. Das Steuerelement schlägt fehl, wenn die Protokollebene des Field Resolvers auf Keine

gesetzt ist. Sofern Sie keine benutzerdefinierten Parameterwerte angeben, um anzugeben, dass ein bestimmter Protokolltyp aktiviert werden soll, erzeugt Security Hub eine erfolgreiche Suche, wenn die Protokollebene des Feldauflösers entweder `ERROR` oder `ALL` ist.

Sie können die Protokollierung und Metriken verwenden, um Ihre GraphQL-Abfragen zu identifizieren, Fehler darin zu beheben und sie zu optimieren. Wenn Sie die Protokollierung für AWS AppSync GraphQL aktivieren, erhalten Sie detaillierte Informationen zu API-Anfragen und -Antworten, können Probleme identifizieren und darauf reagieren und gesetzliche Anforderungen erfüllen.

Abhilfe

Informationen zum Aktivieren der Protokollierung für AWS AppSync finden Sie unter Einrichtung und Konfiguration im AWS AppSync Entwicklerhandbuch.

[AppSync.4] AWS AppSync GraphQL-APIs sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AppSync::GraphQLApi`

AWS Config Regel: `tagged-appsync-graphqlapi` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS AppSync GraphQL-API Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die GraphQL-API keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die GraphQL-API mit keinem Schlüssel gekennzeichnet ist. System-Tags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS AppSync GraphQL-API finden Sie TagResourcein der AWS AppSync API-Referenz.

[AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-6

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Hoch

Art der Ressource: `AWS::AppSync::GraphQLApi`

AWS Config -Regel: `appsync-authorization-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `AllowedAuthorizationTypes: AWS_LAMBDA, AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS` (nicht anpassbar)

Dieses Steuerelement prüft, ob Ihre Anwendung einen API-Schlüssel verwendet, um mit einer AWS AppSync GraphQL-API zu interagieren. Die Steuerung schlägt fehl, wenn eine AWS AppSync GraphQL-API mit einem API-Schlüssel authentifiziert wird.

Ein API-Schlüssel ist ein fest codierter Wert in Ihrer Anwendung, der vom AWS AppSync Dienst generiert wird, wenn Sie einen nicht authentifizierten GraphQL-Endpunkt erstellen. Wenn dieser API-Schlüssel kompromittiert ist, ist Ihr Endpunkt anfällig für unbeabsichtigten Zugriff. Sofern Sie keine öffentlich zugängliche Anwendung oder Website unterstützen, empfehlen wir nicht, einen API-Schlüssel zur Authentifizierung zu verwenden.

Abhilfe

Informationen zum Einrichten einer Autorisierungsoption für Ihre AWS AppSync GraphQL-API finden Sie unter Autorisierung und Authentifizierung im AWS AppSync Entwicklerhandbuch.

Amazon Athena Athena-Steuerung

Diese Kontrollen beziehen sich auf Athena-Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Athena.1] Athena-Arbeitsgruppen sollten im Ruhezustand verschlüsselt werden

> **Important**
>
> Security Hub hat diese Kontrolle im April 2024 eingestellt. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6))

Schweregrad: Mittel

Art der Ressource: `AWS::Athena::WorkGroup`

AWS Config -Regel: `athena-workgroup-encrypted-at-rest`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Athena-Arbeitsgruppe im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn eine Athena-Arbeitsgruppe im Ruhezustand nicht verschlüsselt ist.

In Athena können Sie Arbeitsgruppen erstellen, um Abfragen für Teams, Anwendungen oder verschiedene Workloads auszuführen. Jede Arbeitsgruppe hat eine Einstellung, um die Verschlüsselung für alle Abfragen zu aktivieren. Sie haben die Möglichkeit, serverseitige Verschlüsselung mit von Amazon Simple Storage Service (Amazon S3) verwalteten Schlüsseln, serverseitige Verschlüsselung mit AWS Key Management Service (AWS KMS) -Schlüsseln oder clientseitige Verschlüsselung mit kundenverwalteten KMS-Schlüsseln zu verwenden. Daten im Ruhezustand beziehen sich auf alle Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch Verschlüsselung können Sie die Vertraulichkeit solcher Daten schützen und so das Risiko verringern, dass ein unberechtigter Benutzer darauf zugreifen kann.

Abhilfe

Informationen zum Aktivieren der Verschlüsselung im Ruhezustand für Athena-Arbeitsgruppen finden Sie unter Bearbeiten einer Arbeitsgruppe im Amazon Athena Athena-Benutzerhandbuch. Wählen Sie im Abschnitt Konfiguration der Abfrageergebnisse die Option Abfrageergebnisse verschlüsseln aus.

[Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Athena::DataCatalog`

AWS Config Regel: `tagged-athena-datacatalog` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein Amazon Athena Athena-Datenkatalog Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Datenkatalog keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Datenkatalog mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Athena-Datenkatalog finden Sie unter Tagging Athena-Ressourcen im Amazon Athena Athena-Benutzerhandbuch.

[Athena.3] Athena-Arbeitsgruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Athena::WorkGroup`

AWS Config Regel: `tagged-athena-workgroup` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob eine Amazon Athena Athena-Arbeitsgruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind. `requiredTagKeys` Die Steuerung schlägt fehl, wenn die Arbeitsgruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Arbeitsgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Stichwörtern zu einer Athena-Arbeitsgruppe finden Sie unter Hinzufügen und Löschen von Stichwörtern in einer einzelnen Arbeitsgruppe im Amazon Athena Athena-Benutzerhandbuch.

AWS Backup Steuerungen

Diese Kontrollen beziehen sich auf AWS Backup Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein

Verwandte Anforderungen: NIST.800-53.R5 CP-9 (8), NIST.800-53.R5 SI-12

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: `AWS::Backup::RecoveryPoint`

AWS Config -Regel: `backup-recovery-point-encrypted`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS Backup Wiederherstellungspunkt im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn der Erholungspunkt im Ruhezustand nicht verschlüsselt ist.

Ein AWS Backup Wiederherstellungspunkt bezieht sich auf eine bestimmte Kopie oder einen Snapshot von Daten, der im Rahmen eines Backup-Vorgangs erstellt wird. Er stellt einen bestimmten Zeitpunkt dar, zu dem die Daten gesichert wurden, und dient als Wiederherstellungspunkt für den Fall, dass die Originaldaten verloren gehen, beschädigt werden oder nicht mehr zugänglich sind. Die Verschlüsselung der Backup-Wiederherstellungspunkte bietet zusätzlichen Schutz vor unbefugtem Zugriff. Die Verschlüsselung ist eine bewährte Methode zum Schutz der Vertraulichkeit, Integrität und Sicherheit von Backup-Daten.

Abhilfe

Informationen zur Verschlüsselung eines AWS Backup Wiederherstellungspunkts finden Sie unter Verschlüsselung für Backups AWS Backup im AWS Backup Entwicklerhandbuch.

[Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::Backup::RecoveryPoint`

AWS Config Regel: `tagged-backup-recoverypoint` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Backup Wiederherstellungspunkt über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Erholungspunkt keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Erholungspunkt mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

So fügen Sie einem AWS Backup Recovery Point Tags hinzu

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup-Pläne aus.
3. Wählen Sie einen Backup-Plan aus der Liste aus.
4. Wählen Sie im Abschnitt Backup-Plan-Tags die Option Tags verwalten aus.

5. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wählen Sie Neues Tag hinzufügen für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

[Backup.3] AWS Backup Tresore sollten markiert sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Backup::BackupVault`

AWS Config Regel: `tagged-backup-backupvault` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Backup Tresor Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Recovery Point keine Tag-Schlüssel hat oder wenn er nicht über alle im Parameter angegebenen Schlüssel verfügt`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Erholungspunkt mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

So fügen Sie Tags zu einem Tresor hinzu AWS Backup

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup vaults (Sicherungstresore) aus.
3. Wählen Sie einen Backup-Tresor aus der Liste aus.
4. Wählen Sie im Abschnitt Backup-Tresor-Tags die Option Tags verwalten aus.
5. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wählen Sie Neues Tag hinzufügen für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

[Backup.4] AWS Backup Berichtspläne sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Backup::ReportPlan`

AWS Config Regel: `tagged-backup-reportplan` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Backup Berichtsplan Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn der Berichtsplan keine Tagschlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Berichtsplan mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen

anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

So fügen Sie Stichwörter zu einem Berichtsplan AWS Backup hinzu

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup vaults (Sicherungstresore) aus.
3. Wählen Sie einen Backup-Tresor aus der Liste aus.
4. Wählen Sie im Abschnitt Backup-Tresor-Tags die Option Tags verwalten aus.
5. Wählen Sie Neues Tag hinzufügen aus. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wiederholen Sie den Vorgang für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

[Backup.5] AWS Backup Backup-Pläne sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Backup::BackupPlan`

AWS Config Regel: `tagged-backup-backupplan` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Backup Backup-Plan Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn der Backup-Plan keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Backup-Plan mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

So fügen Sie Tags zu einem Backup-Plan AWS Backup hinzu

1. Öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup vaults (Sicherungstresore) aus.
3. Wählen Sie einen Backup-Tresor aus der Liste aus.
4. Wählen Sie im Abschnitt Backup-Tresor-Tags die Option Tags verwalten aus.
5. Wählen Sie Neues Tag hinzufügen aus. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wiederholen Sie den Vorgang für weitere Schlüssel-Wert-Paare.
6. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

AWS CloudFormation steuert

Diese Kontrollen beziehen sich auf CloudFormation Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[CloudFormation.1] CloudFormation Stacks sollten in Simple Notification Service (SNS) integriert werden

> **Important**
>
> Security Hub hat diese Kontrolle im April 2024 eingestellt. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: NIST.800-53.R5 SI-4 (12), NIST.800-53.R5 SI-4 (5)

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudFormation::Stack`

AWS Config -Regel: `cloudformation-stack-notification-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob eine Amazon Simple Notification Service-Benachrichtigung in einen AWS CloudFormation Stack integriert ist. Die Kontrolle schlägt für einen CloudFormation Stack fehl, wenn ihm keine SNS-Benachrichtigung zugeordnet ist.

Wenn Sie eine SNS-Benachrichtigung mit Ihrem CloudFormation Stack konfigurieren, können Sie die Beteiligten sofort über alle Ereignisse oder Änderungen informieren, die im Stack auftreten.

Abhilfe

Informationen zur Integration eines CloudFormation Stacks und eines SNS-Themas finden Sie unter Stacks direkt aktualisieren im AWS CloudFormation Benutzerhandbuch.

[CloudFormation.2] CloudFormation Stapel sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudFormation::Stack`

AWS Config Regel: `tagged-cloudformation-stack` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS CloudFormation Stack Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn der Stack keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Stack mit keinem Schlüssel gekennzeichnet ist. System-Tags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem CloudFormation Stack finden Sie CreateStackin der AWS CloudFormation API-Referenz.

CloudFront Amazon-Kontrollen

Diese Kontrollen beziehen sich auf CloudFront Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein

Verwandte Anforderungen: NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16)

Kategorie: Schützen > Sichere Zugriffsverwaltung > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: `cloudfront-default-root-object-configured`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine CloudFront Amazon-Distribution so konfiguriert ist, dass sie ein bestimmtes Objekt zurückgibt, das das Standard-Root-Objekt ist. Die Steuerung schlägt fehl, wenn für die CloudFront Verteilung kein Standard-Stammobjekt konfiguriert ist.

Ein Benutzer kann manchmal die Stamm-URL der Distribution anstelle eines Objekts in der Distribution anfordern. In diesem Fall können Sie durch die Festlegung eines Standardstammobjekt verhindern, dass die Inhalte Ihrer Web-Verteilung preisgegeben werden.

Abhilfe

Informationen zur Konfiguration eines Standard-Root-Objekts für eine CloudFront Distribution finden Sie unter How to specify a default root object im Amazon CloudFront Developer Guide.

[CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen

Verwandte Anforderungen: NIST.800-53.R5 AC-17 (2), NIST.800-53.R5 AC-4, NIST.800-53.R5 IA-5 (1), NIst.800-53.R5 SC-12 (3), NIst.800-53.R5 SC-13, NIst.800-53.R5 SC-23, NIst.800-53.R5 SC-23 (3), NIst.NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten währen der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: `cloudfront-viewer-policy-https`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob eine CloudFront Amazon-Distribution verlangt, dass Zuschauer HTTPS direkt verwenden, oder ob sie eine Umleitung verwendet. Die Steuerung schlägt fehl, wenn sie auf `allow-all` für `defaultCacheBehavior` oder für `cacheBehaviors` gesetzt `ViewerProtocolPolicy` ist.

HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer person-in-the-middle oder ähnliche Angriffe verwenden, um den Netzwerkverkehr zu belauschen oder zu manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Die Verschlüsselung von Daten während der Übertragung kann die Leistung beeinträchtigen. Sie sollten Ihre Anwendung mit dieser Funktion testen, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen.

Abhilfe

Informationen zum Verschlüsseln einer CloudFront Verteilung während der Übertragung finden Sie unter HTTPS für die Kommunikation zwischen Zuschauern erforderlich und CloudFront im Amazon CloudFront Developer Guide.

[CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: `cloudfront-origin-failover-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob eine CloudFront Amazon-Distribution mit einer Ursprungsgruppe konfiguriert ist, die zwei oder mehr Ursprünge hat.

CloudFront Origin-Failover kann die Verfügbarkeit erhöhen. Origin-Failover leitet den Datenverkehr automatisch an einen sekundären Ursprung weiter, wenn der primäre Ursprung nicht verfügbar ist oder wenn bestimmte HTTP-Antwortstatuscodes zurückgegeben werden.

Abhilfe

Informationen zur Konfiguration des Origin-Failovers für eine CloudFront Distribution finden Sie unter Creating an Origin Group im Amazon CloudFront Developer Guide.

[CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.r5 AU-3 R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: `cloudfront-accesslogs-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Serverzugriffsprotokollierung für CloudFront Distributionen aktiviert ist. Die Steuerung schlägt fehl, wenn die Zugriffsprotokollierung für eine Verteilung nicht aktiviert ist.

CloudFront Zugriffsprotokolle enthalten detaillierte Informationen über jede eingehende Benutzeranfrage CloudFront . Jedes Protokoll enthält Informationen wie Datum und Uhrzeit des Eingangs der Anfrage, die IP-Adresse des Betrachters, der die Anfrage gestellt hat, die Quelle der Anfrage und die Portnummer der Anfrage vom Betrachter.

Diese Protokolle sind für Anwendungen wie Sicherheits- und Zugriffsprüfungen sowie forensische Untersuchungen nützlich. Weitere Hinweise zur Analyse von Zugriffsprotokollen finden Sie unter Abfragen von CloudFront Amazon-Protokollen im Amazon Athena-Benutzerhandbuch.

Abhilfe

Informationen zur Konfiguration der Zugriffsprotokollierung für eine CloudFront Distribution finden Sie unter Konfiguration und Verwendung von Standardprotokollen (Zugriffsprotokollen) im Amazon CloudFront Developer Guide.

[CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-4 (21)

Kategorie: Schützen > Schutzdienste

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: `cloudfront-associated-with-waf`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob CloudFront Distributionen entweder AWS WAF Classic- oder AWS WAF Web-ACLs zugeordnet sind. Das Steuerelement schlägt fehl, wenn die Verteilung keiner Web-ACL zugeordnet ist.

AWS WAF ist eine Firewall für Webanwendungen, die dazu beiträgt, Webanwendungen und APIs vor Angriffen zu schützen. Sie ermöglicht es ihnen, eine Gruppe von Regeln (eine sogenannte Web-Zugriffskontrollliste oder Web-ACL) zum Zulassen, Blockieren oder Zählen von Webanforderungen basierend auf von Ihnen definierten anpassbaren Web-Sicherheitsregeln und Bedingungen zu konfigurieren. Stellen Sie sicher, dass Ihre CloudFront Distribution mit einer AWS WAF Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Abhilfe

Informationen zum Verknüpfen einer AWS WAF Web-ACL mit einer CloudFront Distribution finden Sie unter Verwendung AWS WAF zur Zugriffskontrolle auf Ihre Inhalte im Amazon CloudFront Developer Guide.

[CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden

Verwandte Anforderungen: NIST.800-53.R5 AC-17 (2), NIST.800-53.R5 AC-4, NIST.800-53.R5 IA-5 (1), NIst.800-53.R5 SC-12 (3), NIst.800-53.R5 SC-13, NIst.800-53.R5 SC-23, NIst.800-53.R5 SC-23 (3), NIst.NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: `cloudfront-custom-ssl-certificate`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob CloudFront Distributionen die standardmäßigen SSL-/TLS-Zertifikate verwenden. CloudFront Diese Kontrolle ist erfolgreich, wenn die CloudFront Distribution ein

benutzerdefiniertes SSL/TLS-Zertifikat verwendet. Diese Kontrolle schlägt fehl, wenn die CloudFront Verteilung das standardmäßige SSL/TLS-Zertifikat verwendet.

Benutzerdefiniertes SSL/TLS ermöglicht Ihren Benutzern den Zugriff auf Inhalte mithilfe alternativer Domainnamen. Sie können benutzerdefinierte Zertifikate in AWS Certificate Manager (empfohlen) oder in IAM speichern.

Abhilfe

Informationen zum Hinzufügen eines alternativen Domainnamens für eine CloudFront Distribution mit einem benutzerdefinierten SSL/TLS-Zertifikat finden Sie unter Hinzufügen eines alternativen Domainnamens im Amazon CloudFront Developer Guide.

[CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: `cloudfront-sni-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob CloudFront Amazon-Distributionen ein benutzerdefiniertes SSL/TLS-Zertifikat verwenden und so konfiguriert sind, dass sie SNI für die Bearbeitung von HTTPS-Anfragen verwenden. Diese Kontrolle schlägt fehl, wenn ein benutzerdefiniertes SSL/TLS-Zertifikat zugeordnet ist, die SSL/TLS-Unterstützungsmethode jedoch eine dedizierte IP-Adresse ist.

Die Servernamensanzeige (SNI) ist eine Erweiterung des TLS-Protokolls, die in Browsern und Clients unterstützt wird, die nach 2010 veröffentlicht wurden. Wenn Sie so konfigurieren CloudFront , dass HTTPS-Anfragen mithilfe von SNI bedient werden, verknüpfen Sie CloudFront Ihren alternativen Domainnamen mit einer IP-Adresse für jeden Edge-Standort. Sobald ein Viewer Inhalte von Ihnen durch Senden einer HTTPS-Anforderung abruft, leitet DNS die Anforderung an die IP-Adresse des korrekten Edge-Standorts weiter. Die IP-Adresse für Ihren Domänennamen wird während der SSL-/TLS-Handshake-Aushandlung bestimmt; die IP-Adresse ist nicht für Ihre Verteilung reserviert.

Abhilfe

Informationen zur Konfiguration einer CloudFront Distribution für die Verwendung von SNI zur Bearbeitung von HTTPS-Anfragen finden Sie unter Verwenden von SNI zur Bearbeitung von HTTPS-Anfragen (funktioniert für die meisten Kunden) im CloudFront Entwicklerhandbuch.

[CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln

Verwandte Anforderungen: NIST.800-53.R5 AC-17 (2), NIST.800-53.R5 AC-4, NIST.800-53.R5 IA-5 (1), NIst.800-53.R5 SC-12 (3), NIst.800-53.R5 SC-13, NIst.800-53.R5 SC-23, NIst.800-53.R5 SC-23 (3), NIst.NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: `cloudfront-traffic-to-origin-encrypted`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob CloudFront Amazon-Distributionen den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln. Diese Kontrolle schlägt bei einer CloudFront Distribution fehl, deren Ursprungsprotokollrichtlinie „Nur HTTP“ zulässt. Diese Kontrolle schlägt auch fehl, wenn die Ursprungsprotokollrichtlinie der Distribution „Match-Viewer“ lautet, während die Viewer-Protokollrichtlinie „Allow-all“ lautet.

HTTPS (TLS) kann verwendet werden, um das Abhören oder Manipulieren des Netzwerkverkehrs zu verhindern. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden.

Abhilfe

Informationen zur Aktualisierung der Origin-Protokollrichtlinie, sodass für eine CloudFront Verbindung eine Verschlüsselung erforderlich ist, finden Sie im Amazon CloudFront Developer Guide unter HTTPS für die Kommunikation zwischen CloudFront und Ihrem benutzerdefinierten Ursprung erforderlich machen.

[CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden

Verwandte Anforderungen: NIst.800-53.R5 AC-17 (2), NIST.800-53.R5 AC-4, NIST.800-53.R5 IA-5 (1), NIst.800-53.R5 SC-12 (3), NIST.800-53.R5 SC-13, NIst.800-53.R5 SC-23, NIst.800-53.R5 SC-7 (4), NIst.NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: `cloudfront-no-deprecated-ssl-protocols`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob CloudFront Amazon-Distributionen veraltete SSL-Protokolle für die HTTPS-Kommunikation zwischen CloudFront Edge-Standorten und Ihren benutzerdefinierten Ursprüngen verwenden. Diese Kontrolle schlägt fehl, wenn eine CloudFront Distribution über ein Where Includes verfügt`CustomOriginConfig`. `OriginSslProtocols` `SSLv3`

Im Jahr 2015 gab die Internet Engineering Task Force (IETF) offiziell bekannt, dass SSL 3.0 nicht mehr unterstützt werden sollte, da das Protokoll nicht ausreichend sicher ist. Es wird empfohlen, TLSv1.2 oder höher für die HTTPS-Kommunikation mit Ihren benutzerdefinierten Ursprüngen zu verwenden.

Abhilfe

Informationen zur Aktualisierung der Origin-SSL-Protokolle für eine CloudFront Distribution finden Sie unter HTTPS für die Kommunikation zwischen CloudFront und Ihrem benutzerdefinierten Ursprung erforderlich im Amazon CloudFront Developer Guide.

[CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen

Verwandte Anforderungen: NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: `cloudfront-s3-origin-non-existent-bucket`

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob CloudFront Amazon-Distributionen auf nicht existierende Amazon S3-Ursprünge verweisen. Die Kontrolle schlägt bei einer CloudFront Distribution fehl, wenn der Ursprung so konfiguriert ist, dass er auf einen nicht existierenden Bucket verweist. Diese Steuerung gilt nur für CloudFront Distributionen, bei denen ein S3-Bucket ohne statisches Website-Hosting der S3-Ursprung ist.

Wenn eine CloudFront Distribution in Ihrem Konto so konfiguriert ist, dass sie auf einen nicht existierenden Bucket verweist, kann ein böswilliger Dritter den Bucket erstellen, auf den verwiesen wird, und seine eigenen Inhalte über Ihre Distribution bereitstellen. Wir empfehlen, alle Ursprünge unabhängig vom Routing-Verhalten zu überprüfen, um sicherzustellen, dass Ihre Distributionen auf die richtigen Ursprünge verweisen.

Abhilfe

Informationen zum Ändern einer CloudFront Distribution, sodass sie auf einen neuen Ursprung verweist, finden Sie unter Aktualisieren einer Distribution im Amazon CloudFront Developer Guide.

[CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden

Kategorie: Schützen > Sicheres Zugriffsmanagement > Konfiguration der Ressourcenrichtlinien

Schweregrad: Mittel

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config -Regel: `cloudfront-s3-origin-access-control-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob für eine CloudFront Amazon-Distribution mit einem Amazon S3-Ursprung die Origin Access Control (OAC) konfiguriert ist. Die Kontrolle schlägt fehl, wenn OAC nicht für die CloudFront Distribution konfiguriert ist.

Wenn Sie einen S3-Bucket als Ursprung für Ihre CloudFront Distribution verwenden, können Sie OAC aktivieren. Dies ermöglicht den Zugriff auf den Inhalt im Bucket nur über die angegebene CloudFront Distribution und verhindert den direkten Zugriff aus dem Bucket oder einer anderen Distribution. Obwohl Origin Access Identity (OAI) CloudFront unterstützt wird, bietet OAC zusätzliche Funktionen, und Distributionen, die OAI verwenden, können zu OAC migriert werden. OAI bietet zwar eine sichere Möglichkeit, auf S3-Ursprünge zuzugreifen, weist jedoch Einschränkungen auf, z. B. mangelnde Unterstützung für detaillierte Richtlinienkonfigurationen und für HTTP/HTTPS-Anfragen, die die POST-Methode verwenden und für die Signature Version 4 (Sigv4) erforderlich ist. AWS-Regionen AWS OAI unterstützt auch keine Verschlüsselung mit. AWS Key Management Service OAC basiert auf einer AWS bewährten Methode zur Verwendung von IAM-Dienstprinzipalen zur Authentifizierung mit S3-Ursprüngen.

Abhilfe

Informationen zur Konfiguration von OAC für eine CloudFront Distribution mit S3-Ursprüngen finden Sie unter Beschränken des Zugriffs auf einen Amazon S3 S3-Ursprung im Amazon CloudFront Developer Guide.

[CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudFront::Distribution`

AWS Config Regel: `tagged-cloudfront-distribution` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine CloudFront Amazon-Distribution Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn die Distribution keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Verteilung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer CloudFront Distribution finden Sie unter Tagging CloudFront Amazon-Distributionen im Amazon CloudFront Developer Guide.

AWS CloudTrail Steuerungen

Diese Kontrollen beziehen sich auf CloudTrail Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/2.1, CIS Foundations Benchmark v1.4.0/3.1, CIS AWS Foundations Benchmark v3.0.0/3.1, NIst.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIst.800-53.R5 AU-10, NIst.800-53.r5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 AU-14 (1), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SIR -3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), NIST.800-53.R5 SA-8 (22) AWS

Kategorie: Identifizieren > Protokollierung

Schweregrad: Hoch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `multi-region-cloudtrail-enabled`

Art des Zeitplans: Periodisch

Parameter:

- `readWriteType`: `ALL` (nicht anpassbar)

  `includeManagementEvents`: `true` (nicht anpassbar)

Dieses Steuerelement prüft, ob es mindestens einen multiregionalen AWS CloudTrail Trail gibt, der Lese- und Schreibverwaltungsereignisse erfasst. Das Steuerelement schlägt fehl, wenn es deaktiviert CloudTrail ist oder wenn es nicht mindestens einen CloudTrail Pfad gibt, der Lese- und Schreibverwaltungsereignisse erfasst.

AWS CloudTrail zeichnet AWS API-Aufrufe für Ihr Konto auf und übermittelt Ihnen Protokolldateien. Die aufgezeichneten Informationen umfassen die folgenden Informationen:

- Identität des API-Aufrufers
- Zeit des API-Aufrufs
- Quell-IP-Adresse des API-Aufrufers
- Anforderungsparameter
- Antwortelemente, die von zurückgegeben wurden AWS-Service

CloudTrail bietet eine Historie der AWS API-Aufrufe für ein Konto, einschließlich API-Aufrufen, die über die AWS SDKs AWS Management Console und Befehlszeilentools getätigt wurden. Die Historie umfasst auch API-Aufrufe von höheren Ebenen AWS-Services wie. AWS CloudFormation

Der von erstellte AWS API-Aufrufverlauf CloudTrail ermöglicht Sicherheitsanalysen, die Nachverfolgung von Ressourcenänderungen und die Überprüfung der Einhaltung von Vorschriften. Multi-Regions-Trails bieten auch die folgenden Vorteile.

- Ein Multi-Regions-Trail hilft, unerwartete Aktivitäten zu erkennen, die in ansonsten nicht verwendeten Regionen auftreten.
- Ein Multi-Regions-Trail stellt sicher, dass Global Service Event Logging standardmäßig für einen Trail aktiviert ist. Die globale Protokollierung von Serviceereignissen zeichnet Ereignisse auf, die von AWS globalen Diensten generiert wurden.
- Bei einem Trail mit mehreren Regionen stellen Verwaltungsereignisse für alle Lese- und Schreibvorgänge sicher, dass Verwaltungsvorgänge für alle Ressourcen in einem CloudTrail AWS-Konto aufgezeichnet werden.

Standardmäßig handelt es sich bei CloudTrail Pfaden, die mit dem AWS Management Console erstellt wurden, um Wanderwege mit mehreren Regionen.

Abhilfe

Informationen zum Erstellen eines neuen Wanderweges mit mehreren Regionen finden Sie unter Erstellen eines Wanderweges im AWS CloudTrail Benutzerhandbuch. CloudTrail Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Zusätzliche Einstellungen, Überprüfung der Protokolldatei	Aktiviert
Wählen Sie Protokollereignisse, Verwaltungsereignisse, API-Aktivität	Lesen und Schreiben. Deaktivieren Sie die Kontrollkästchen für Ausnahmen.

Informationen zum Aktualisieren eines vorhandenen Pfads finden Sie unter Aktualisieren eines Pfads im AWS CloudTrail Benutzerhandbuch. Wählen Sie unter Verwaltungsereignisse für API-Aktivität die Optionen Lesen und Schreiben aus.

[CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

Verwandte Anforderungen: PCI DSS v3.2.1/3.4, CIS AWS Foundations Benchmark v1.2.0/2.7, CIS Foundations Benchmark v1.4.0/3.7, CIS AWS Foundations Benchmark v3.0.0/3.5, NIST.800-53.R5 AU-9, NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6) AWS

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::CloudTrail::Trail`

AWS Config -Regel: `cloud-trail-encryption-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob CloudTrail es für die Verwendung der serverseitigen Verschlüsselung (SSE) AWS KMS key konfiguriert ist. Das Steuerelement schlägt fehl, wenn das `KmsKeyId` nicht definiert ist.

Für eine zusätzliche Sicherheitsebene für Ihre vertraulichen CloudTrail Protokolldateien sollten Sie die serverseitige Verschlüsselung mit AWS KMS keys (SSE-KMS) für Ihre CloudTrail Protokolldateien für die Verschlüsselung im Ruhezustand verwenden. Beachten Sie, dass die Protokolldateien, die CloudTrail an Ihre Buckets gesendet werden, standardmäßig durch serverseitige Amazon-Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) verschlüsselt werden.

Abhilfe

Informationen zur Aktivierung der SSE-KMS-Verschlüsselung für CloudTrail Protokolldateien finden Sie unter Aktualisieren eines Pfads zur Verwendung eines KMS-Schlüssels im Benutzerhandbuch.AWS CloudTrail

[CloudTrail.3] Mindestens ein CloudTrail Trail sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v3.2.1/10.1, PCI DSS v3.2.1/10.2.1, PCI DSS v3.2.1/10.2.2, PCI DSS v3.2.1/10.2.3, PCI DSS v3.2.1/10.2.4, PCI DSS v3.2.1/10.2.5, PCI DSS v3.2.1/10.2.6, PCI DSS v3.2.1/10.2.7, PCI DSS v3.2.1/10.3.1, PCI DSS v3.2.1/10.3.2, PCI DSS v3.2.1/10.3.3, PCI DSS v3.2.1/10.3.4, PCI DSS v3.2.1/10.3.5, PCI DSS v3.2.1/10.3.6

Kategorie: Identifizieren > Protokollierung

Schweregrad: Hoch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `cloudtrail-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob in Ihrem ein AWS CloudTrail Trail aktiviert ist AWS-Konto. Die Kontrolle schlägt fehl, wenn für Ihr Konto nicht mindestens ein CloudTrail Trail aktiviert ist.

Einige AWS Dienste ermöglichen jedoch nicht die Protokollierung aller APIs und Ereignisse. Sie sollten alle zusätzlichen Prüfpfade einrichten, mit CloudTrail Ausnahme der Dokumentation der einzelnen Dienste CloudTrail unter Unterstützte Dienste und Integrationen.

Abhilfe

Informationen zu den ersten CloudTrail Schritten und zur Erstellung eines Trails finden Sie im AWS CloudTrail Tutorial Erste Schritte mit im AWS CloudTrail Benutzerhandbuch.

[CloudTrail.4] Die Überprüfung der CloudTrail Protokolldatei sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v3.2.1/10.5.2, PCI DSS v3.2.1/10.5.5, CIS AWS Foundations Benchmark v1.2.0/2.2, CIS Foundations Benchmark v1.4.0/3.2, CIS Foundations Benchmark v3.0.0/3.2, NIST.800-53.R5 AU-9, NIST.800-53.R5 SI-4, NIst.800-53.r5 SI-7 (1), NIST.800-53.r5 SI-7 (1) 7 (3), NIST.800-53.R5 SI-7 (7) AWS AWS

Kategorie: Datenschutz > Datenintegrität

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudTrail::Trail`

AWS Config -Regel: `cloud-trail-log-file-validation-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement überprüft in einem CloudTrail Trail, ob die Integritätsprüfung der Protokolldatei aktiviert ist.

CloudTrail Bei der Überprüfung der Protokolldatei wird eine digital signierte Digest-Datei erstellt, die einen Hash jedes Protokolls enthält, das in Amazon S3 CloudTrail geschrieben wird. Sie können diese Digest-Dateien verwenden, um festzustellen, ob eine Protokolldatei nach CloudTrail der Übermittlung des Protokolls geändert, gelöscht oder unverändert wurde.

Security Hub empfiehlt, dass Sie die Dateiüberprüfung auf allen Wegen aktivieren. Die Protokolldateivalidierung bietet zusätzliche Integritätsprüfungen von CloudTrail Protokollen.

Abhilfe

Informationen zum Aktivieren der CloudTrail Protokolldateivalidierung finden Sie unter Aktivieren der Überprüfung der Integrität von AWS CloudTrail Protokolldateien CloudTrail im Benutzerhandbuch.

[CloudTrail.5] CloudTrail Trails sollten in Amazon CloudWatch Logs integriert werden

Verwandte Anforderungen: PCI DSS v3.2.1/10.5.3, CIS AWS Foundations Benchmark v1.2.0/2.4, CIS Foundations Benchmark v1.4.0/3.4, NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26),

NIST.800-53.R5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-6 (1), NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 AU-7 (1), NIST.800-53.r5 AU-7 (1), NIST.800-53.r5 AU-7 (1) NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-20, NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-4 (AWS 5), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudTrail::Trail`

AWS Config -Regel: `cloud-trail-cloud-watch-logs-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob CloudTrail Trails so konfiguriert sind, dass sie Logs an CloudWatch Logs senden. Die Steuerung schlägt fehl, wenn die `CloudWatchLogsLogGroupArn` Eigenschaft des Trails leer ist.

CloudTrail zeichnet AWS API-Aufrufe auf, die in einem bestimmten Konto getätigt werden. Die aufgezeichneten Informationen umfassen Folgendes:

- Die Identität des API-Aufrufers
- Die Uhrzeit des API-Aufrufs
- Die Quell-IP-Adresse des API-Aufrufers
- Die Anforderungsparameter
- Die Antwortelemente, die von der zurückgegeben wurden AWS-Service

CloudTrail verwendet Amazon S3 für die Speicherung und Lieferung von Protokolldateien. Sie können CloudTrail Protokolle für langfristige Analysen in einem bestimmten S3-Bucket erfassen. Um Echtzeitanalysen durchzuführen, können Sie so konfigurieren, dass CloudWatch Protokolle CloudTrail an Logs gesendet werden.

CloudTrail Sendet bei einem Trail, der in allen Regionen eines Kontos aktiviert ist, Protokolldateien aus all diesen Regionen an eine CloudWatch Logs-Protokollgruppe.

Security Hub empfiehlt, dass Sie CloudTrail CloudWatch Protokolle an Logs senden. Beachten Sie, dass mit dieser Empfehlung sichergestellt werden soll, dass Kontoaktivitäten erfasst, überwacht und entsprechend alarmiert werden. Sie können CloudWatch Logs verwenden, um dies mit Ihrem AWS-Services einzurichten. Diese Empfehlung schließt die Verwendung einer anderen Lösung nicht aus.

Das Senden von CloudTrail CloudWatch Protokollen an Logs ermöglicht die Protokollierung von Aktivitäten in Echtzeit und im Verlauf auf der Grundlage von Benutzer, API, Ressource und IP-Adresse. Mit diesem Ansatz können Sie Alarme und Benachrichtigungen für ungewöhnliche oder sensible Kontoaktivitäten einrichten.

Abhilfe

Informationen zur Integration CloudTrail mit CloudWatch Logs finden Sie im AWS CloudTrail Benutzerhandbuch unter Ereignisse an CloudWatch Logs senden.

[CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/2.3, CIS Foundations Benchmark v1.4.0/3.3 AWS

Kategorie: Identifizieren > Protokollierung

Schweregrad: Kritisch

Art der Ressource: `AWS::S3::Bucket`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Periodisch und durch Änderung ausgelöst

Parameter: Keine

CloudTrail protokolliert eine Aufzeichnung jedes API-Aufrufs, der in Ihrem Konto getätigt wurde. Diese Protokolldateien werden in einem S3-Bucket gespeichert. CIS empfiehlt, die S3-Bucket-Richtlinie oder Zugriffskontrollliste (ACL) auf den S3-Bucket anzuwenden, der CloudTrail protokolliert, um den öffentlichen Zugriff auf die CloudTrail Protokolle zu verhindern. Wenn der öffentliche Zugriff auf CloudTrail Protokollinhalte gewährt wird, kann dies einem Angreifer dabei helfen, Schwachstellen in der Nutzung oder Konfiguration des betroffenen Kontos zu erkennen.

Um diese Prüfung durchzuführen, verwendet Security Hub zunächst benutzerdefinierte Logik, um nach dem S3-Bucket zu suchen, in dem Ihre CloudTrail Logs gespeichert sind. Anschließend überprüft es anhand der AWS Config verwalteten Regeln, ob der Bucket öffentlich zugänglich ist.

Wenn Sie Ihre Logs in einem einzigen zentralen S3-Bucket zusammenfassen, führt Security Hub die Prüfung nur für das Konto und die Region durch, in der sich der zentrale S3-Bucket befindet. Für andere Konten und Regionen lautet der Kontrollstatus Keine Daten.

Wenn der Bucket öffentlich zugänglich ist, generiert die Prüfung einen Fehlschlag.

Abhilfe

Informationen zum Blockieren des öffentlichen Zugriffs auf Ihren CloudTrail S3-Bucket finden Sie unter Konfiguration der Einstellungen zum Sperren des öffentlichen Zugriffs für Ihre S3-Buckets im Amazon Simple Storage Service-Benutzerhandbuch. Wählen Sie alle vier Amazon S3 Block Public Access-Einstellungen aus.

[CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/2.6, CIS Foundations Benchmark v1.4.0/3.6, CIS AWS Foundations Benchmark v3.0.0/3.4 AWS

Kategorie: Identifizieren > Protokollierung

Schweregrad: Niedrig

Art der Ressource: `AWS::S3::Bucket`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Die S3-Bucket-Zugriffsprotokollierung generiert ein Protokoll, das Zugriffsdatensätze für jede Anfrage an Ihren S3-Bucket enthält. Ein Zugriffsprotokoll-Datensatz enthält Details über jede Anfrage, wie beispielsweise den Anforderungstyp, die in der Anfrage angeforderten Ressource sowie Uhrzeit und Datum der Anfrage.

CIS empfiehlt, die Bucket-Zugriffsprotokollierung für den CloudTrail S3-Bucket zu aktivieren.

Durch das Aktivieren der S3-Bucket-Protokollierung für Ziel-S3-Buckets können Sie alle Ereignisse erfassen, die Auswirkungen auf Objekte in einem Ziel-Bucket haben können. Wenn Protokolle so konfiguriert sind, dass sie in einem separaten Bucket platziert werden, haben Sie Zugang zu Protokollinformationen, die in Sicherheits- und Vorfallreaktions-Workflows hilfreich sein können.

Um diese Prüfung durchzuführen, verwendet Security Hub zunächst benutzerdefinierte Logik, um nach dem Bucket zu suchen, in dem Ihre CloudTrail Protokolle gespeichert sind, und verwendet dann die AWS Config verwaltete Regel, um zu überprüfen, ob die Protokollierung aktiviert ist.

Wenn CloudTrail Protokolldateien von mehreren AWS-Konten in einen einzigen Amazon S3 S3-Ziel-Bucket übertragen werden, wertet Security Hub diese Kontrolle nur anhand des Ziel-Buckets in der Region aus, in der er sich befindet. Dadurch werden Ihre Ergebnisse optimiert. Sie sollten diese Option jedoch CloudTrail in allen Konten aktivieren, die Logs an den Ziel-Bucket senden. Für alle Konten außer dem Konto, das den Ziel-Bucket enthält, lautet der Kontrollstatus Keine Daten.

Wenn der Bucket öffentlich zugänglich ist, generiert die Prüfung einen Fehler.

Abhilfe

Informationen zum Aktivieren der Serverzugriffsprotokollierung für Ihren CloudTrail S3-Bucket finden Sie unter Aktivieren der Amazon S3 S3-Serverzugriffsprotokollierung im Amazon Simple Storage Service-Benutzerhandbuch.

[CloudTrail.9] CloudTrail Pfade sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CloudTrail::Trail`

AWS Config Regel: `tagged-cloudtrail-trail` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein AWS CloudTrail Trail Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn der Trail keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Trail mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem CloudTrail Trail finden Sie AddTagsin der AWS CloudTrail API-Referenz.

CloudWatch Amazon-Kontrollen

Diese Kontrollen beziehen sich auf CloudWatch Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[CloudWatch.1] Für den Benutzer „root“ sollten ein Metrik-Logfilter und ein Alarm vorhanden sein

Verwandte Anforderungen: PCI DSS v3.2.1/7.2.1, CIS AWS Foundations Benchmark v1.2.0/1.1, CIS Foundations Benchmark v1.2.0/3.3, CIS Foundations Benchmark v1.4.0/1.7, CIS AWS Foundations Benchmark v1.4.0/4.3 AWS AWS

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

`AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::Trail`Ressourcentyp:,,, `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Der Root-Benutzer hat uneingeschränkten Zugriff auf alle Dienste und Ressourcen in einem AWS-Konto. Wir empfehlen dringend, den Root-Benutzer nicht für tägliche Aufgaben zu verwenden.

Durch die Minimierung der Nutzung des Root-Benutzers und die Anwendung des Prinzips der geringsten Rechte für die Zugriffsverwaltung wird das Risiko unbeabsichtigter Änderungen und der unbeabsichtigten Offenlegung hochberechtigter Anmeldeinformationen verringert.

Es hat sich bewährt, Ihre Root-Benutzeranmeldedaten nur dann zu verwenden, wenn sie für die Durchführung von Konto- und Dienstverwaltungsaufgaben erforderlich sind. Wenden Sie AWS Identity and Access Management (IAM-) Richtlinien direkt auf Gruppen und Rollen an, aber nicht auf Benutzer. Ein Tutorial zur Einrichtung eines Administrators für den täglichen Gebrauch finden Sie im IAM-Benutzerhandbuch unter Erstellen Ihres ersten IAM-Admin-Benutzers und Ihrer ersten Gruppe

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 1.7 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

> **Note**
>
> Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.
> Die Prüfung führt in den folgenden Fällen zu `FAILED` Ergebnissen:
>
> - Es ist kein Trail konfiguriert.
> - Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.
>
> Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:
>
> - Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
> - Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.
>
>   Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten

Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT`

Feld	Value (Wert)
	`EXISTS && $.eventType !="AwsServiceEvent"}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Größer/Gleich
als...	**`1`**

[CloudWatch.2] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.1

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp:`AWS::Logs::MetricFilter`,,, `AWS::CloudWatch::Alarm` `AWS::CloudTrail::Trail` `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch

CIS empfiehlt, einen metrischen Filter zu erstellen und unberechtigte API-Aufrufe zu alarmieren. Die Überwachung nicht autorisierter API-Aufrufe hilft, Anwendungsfehler aufzudecken, und kann die Erkennung böswilliger Aktivitäten beschleunigen.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 3.1 im CIS AWS Foundations Benchmark v1.2 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.
Die Prüfung führt in den folgenden Fällen zu `FAILED` Ergebnissen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub

nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.errorCode="*UnauthorizedOperation") \|\| ($.errorCode="AccessDenied*")}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**

Feld	Value (Wert)
Standardwert	**0**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *your-metric-name* ist...	Größer/Gleich
als...	**1**

[CloudWatch.3] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Anmeldung an der Management Console ohne MFA vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.2

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp:`AWS::Logs::MetricFilter`,, `AWS::CloudWatch::Alarm` `AWS::CloudTrail::Trail` `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch

CIS empfiehlt, einen Metrikfilter und Alarm-Konsolen-Logins zu erstellen, die nicht durch MFA geschützt sind. Durch die Überwachung zur Feststellung von Single-Factor-Konsolenanmeldungen wird die Transparenz im Hinblick auf Konten ohne MFA-Schutz gesteigert.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 3.2 im CIS AWS Foundations Benchmark v1.2 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

> **Note**
>
> Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.
> Die Prüfung führt in den folgenden Fällen zu `FAILED` Ergebnissen:
>
> - Es ist kein Trail konfiguriert.
> - Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.
>
> Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:
>
> - Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
> - Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.
>
>   Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") && ($.userIdentity.type = "IAMUser") && ($.responseElements.ConsoleLogin = "Success") }`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**

Feld	Value (Wert)
Standardwert	**0**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *your-metric-name* ist...	Größer/Gleich
als...	**1**

[CloudWatch.4] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für IAM-Richtlinienänderungen vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.4, CIS Foundations Benchmark v1.4.0/4.4 AWS

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp:,, `AWS::Logs::MetricFilter` `AWS::CloudWatch::Alarm` `AWS::CloudTrail::Trail` `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Sie API-Aufrufe in Echtzeit überwachen, indem es CloudTrail CloudWatch Protokolle an Logs weiterleitet und entsprechende Metrikfilter und Alarme einrichtet.

CIS empfiehlt, einen Metrikfilter und einen Alarm für Änderungen an den IAM-Richtlinien zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass Authentifizierungs- und Autorisierungskontrollen intakt bleiben.

Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.
Die Prüfung führt in den folgenden Fällen zu `FAILED` Ergebnissen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

> **Note**
>
> Unser empfohlenes Filtermuster für diese Behebungsschritte unterscheidet sich von dem Filtermuster in den CIS-Leitlinien. Unsere empfohlenen Filter zielen nur auf Ereignisse ab, die aus IAM-API-Aufrufen stammen.

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventSource=iam.amazonaws.com) && (($.eventName=DeleteGroupPolicy) || ($.eventName=DeleteRolePolicy) \|\| ($.eventName=DeleteUserPolicy) || ($.eventName=PutGroupPolicy) \|\| ($.eventName=PutRolePolicy) || ($.eventName=PutUserPolicy) \|\| ($.eventName=CreatePolicy) || ($.eventName=DeletePolicy) \|\| ($.eventName=Creat`

Feld	Value (Wert)
	`ePolicyVersion) || ($.eventName=DeletePolicyVersion) \|\| ($.eventName=AttachRolePolicy) || ($.eventName=DetachRolePolicy) \|\| ($.eventName=AttachUserPolicy) || ($.eventName=DetachUserPolicy) \|\| ($.eventName=AttachGroupPolicy) || ($.eventName=DetachGroupPolicy))}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Größer/Gleich
als...	**`1`**

[CloudWatch1.5] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der Dauer CloudTrail AWS Config vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.5, CIS Foundations Benchmark v1.4.0/4.5 AWS

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp:,, `AWS::Logs::MetricFilter` `AWS::CloudWatch::Alarm` `AWS::CloudTrail::Trail` `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch

CIS empfiehlt, einen metrischen Filter und einen Alarm für Änderungen an den CloudTrail Konfigurationseinstellungen zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass die Transparenz für Aktivitäten in diesem Konto erhalten bleibt.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.5 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

> **Note**
>
> Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.
> Die Prüfung führt in den folgenden Fällen zu `FAILED` Ergebnissen:
>
> - Es ist kein Trail konfiguriert.
> - Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.
>
> Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:
>
> - Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.

- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventName=CreateTrail) \|\| ($.eventName=UpdateTrail) || ($.eventName=DeleteTrail) \|\| ($.eventName=StartLogging) || ($.eventName=StopLogging)}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Größer/Gleich
als...	**`1`**

[CloudWatch.6] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.6, CIS Foundations Benchmark v1.4.0/4.6 AWS

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp:,,, `AWS::Logs::MetricFilter` `AWS::CloudWatch::Alarm` `AWS::CloudTrail::Trail` `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch

CIS empfiehlt, einen metrischen Filter und einen Alarm für fehlgeschlagene Konsolenauthentifizierungsversuche zu erstellen. Durch die Überwachung fehlgeschlagenere Konsolenanmeldungen kann die Vorlaufzeit für die Erkennung von Brute-Force-Angriffsversuchen auf Anmeldeinformationen reduziert werden, durch die ein Indikator geliefert werden kann (wie z. B. eine Quell-IP), den Sie in anderen Ereigniskorrelationen verwenden können.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.6 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

> **Note**
>
> Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.
> Die Prüfung führt in den folgenden Fällen zu `FAILED` Ergebnissen:
>
> - Es ist kein Trail konfiguriert.
> - Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.
>
> Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:
>
> - Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
> - Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventName=ConsoleLogin) && ($.errorMessage="Failed authentication")}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Größer/Gleich
als...	**`1`**

[CloudWatch.7] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.7, CIS Foundations Benchmark v1.4.0/4.7 AWS

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp:,,, `AWS::Logs::MetricFilter` `AWS::CloudWatch::Alarm` `AWS::CloudTrail::Trail` `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch

CIS empfiehlt, einen Metrikfilter und einen Alarm für vom Kunden verwaltete Schlüssel zu erstellen, deren Status in „Deaktiviert“ oder „Geplantes Löschen“ geändert wurde. Mit deaktivierten oder gelöschten Schlüsseln verschlüsselte Daten sind nicht mehr zugänglich.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.7 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden. Die Steuerung schlägt auch fehl, `ExcludeManagementEventSources` wenn `kms.amazonaws.com`

> **Note**
>
> Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.
> Die Prüfung führt in den folgenden Fällen zu `FAILED` Ergebnissen:
>
> - Es ist kein Trail konfiguriert.
> - Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.
>
> Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:
>
> - Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
> - Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventSource=kms.amazonaws.com) && (($.eventName=DisableKey) || ($.eventName=ScheduleKeyDeletion))}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Größer/Gleich
als...	**`1`**

[CloudWatch.8] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.8, CIS Foundations Benchmark v1.4.0/4.8 AWS

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp:,,, `AWS::Logs::MetricFilter` `AWS::CloudWatch::Alarm` `AWS::CloudTrail::Trail` `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch

CIS empfiehlt, einen Metrikfilter und einen Alarm für Änderungen an den S3-Bucket-Richtlinien zu erstellen. Durch das Überwachen dieser Änderungen können Sie die Zeit reduzieren, die zum Erkennen und Korrigieren permissiver Richtlinien für sensible S3-Buckets erforderlich ist.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.8 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

> **Note**
>
> Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.
> Die Prüfung führt in den folgenden Fällen zu `FAILED` Ergebnissen:
>
> - Es ist kein Trail konfiguriert.
> - Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.
>
> Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:
>
> - Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
> - Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.
>
>   Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können

nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventSource=s3.amazonaws.com) && (($.eventName=PutBucketAcl) || ($.eventName=PutBu`

Feld	Value (Wert)
	`cketPolicy) || ($.eventN ame=PutBucketCors) \|\| ($.eventN ame=PutBucketLifecycle) || ($.eventName=PutBucketRepli cation) \|\| ($.eventName=Delet eBucketPolicy) || ($.eventN ame=DeleteBucketCors) \|\| ($.eventName=DeleteBucketLi fecycle) || ($.eventName=Delet eBucketReplication))}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Größer/Gleich
als...	**`1`**

[CloudWatch.9] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Config Konfigurationsänderungen vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.9, CIS Foundations Benchmark v1.4.0/4.9 AWS

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Ressourcentyp:,,, `AWS::Logs::MetricFilter` `AWS::CloudWatch::Alarm` `AWS::CloudTrail::Trail` `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch

CIS empfiehlt, einen metrischen Filter und einen Alarm für Änderungen an den AWS Config Konfigurationseinstellungen zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass die Transparenz im Hinblick auf Konfigurationselemente in diesem Konto erhalten bleibt.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.9 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

> **Note**
>
> Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.
> Die Prüfung führt in den folgenden Fällen zu `FAILED` Ergebnissen:
>
> - Es ist kein Trail konfiguriert.
> - Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.
>
> Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:
>
> - Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.

- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventSource=config.amazonaws.com) && (($.eventName=StopConfigurationRecorder) || ($.eventName=DeleteDeliveryChannel) \|\| ($.eventName=PutDeliveryChannel) || ($.eventName=PutConfigurationRecorder))}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Größer/Gleich
als...	**`1`**

[CloudWatch.10] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.10, CIS Foundations Benchmark v1.4.0/4.10 AWS

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

`AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::TrailRessourcentyp:,, AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch Sicherheitsgruppen sind ein zustandsorientierter Paketfilter zur Steuerung von ein- und ausgehendem Datenverkehr in einer VPC.

CIS empfiehlt, einen Metrikfilter und einen Alarm für Änderungen an Sicherheitsgruppen zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass -Ressourcen und -Services nicht unbeabsichtigt ungeschützt sind.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Control 4.10 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

> **Note**
>
> Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.
> Die Prüfung führt in den folgenden Fällen zu `FAILED` Ergebnissen:
>
> - Es ist kein Trail konfiguriert.
> - Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.
>
> Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:
>
> - Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.

- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventName=AuthorizeSecurityGroupIngress) \|\| ($.eventName=AuthorizeSecurityGroupEgress) || ($.eventName=RevokeSecurityGroupIngress) \|\| ($.eventName=RevokeSecurityGroupEgress) || ($.eventName=CreateSecurityGroup) \|\| ($.eventName=DeleteSecurityGroup)}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Größer/Gleich
als...	**`1`**

[CloudWatch.11] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.11, CIS Foundations Benchmark v1.4.0/4.11 AWS

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

`AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::TrailRessourcentyp:,, AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch NACLs dienen als zustandslose Paketfilter zur Steuerung von ein- und ausgehendem Datenverkehr für Subnetze in einer VPC.

CIS empfiehlt, einen metrischen Filter und einen Alarm für Änderungen an NACLs zu erstellen. Durch die Überwachung dieser Änderungen wird sichergestellt, dass AWS Ressourcen und Dienste nicht unbeabsichtigt offengelegt werden.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.11 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

> **Note**
>
> Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.
> Die Prüfung führt in den folgenden Fällen zu `FAILED` Ergebnissen:
>
> - Es ist kein Trail konfiguriert.
> - Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventName=CreateNetworkAcl) \|\| ($.eventName=CreateNetworkAclEntry) || ($.eventName=DeleteNetworkAcl) \|\| ($.eventName=DeleteNetworkAclEntry) || ($.eventName=ReplaceNetworkAclEntry) \|\| ($.eventName=ReplaceNetworkAclAssociation)}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Größer/Gleich
als...	**`1`**

[CloudWatch.12] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.12, CIS Foundations Benchmark v1.4.0/4.12 AWS

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

`AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::TrailRessourcentyp:,, AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch Netzwerk-Gateways sind erforderlich, um Datenverkehr an ein Ziel außerhalb einer VPC zu senden und Datenverkehr von einem solchen Ziel zu empfangen.

CIS empfiehlt, einen metrischen Filter und einen Alarm für Änderungen an Netzwerk-Gateways zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass der gesamte eingehende und ausgehende Datenverkehr die VPC-Grenze über einen kontrollierten Pfad durchquert.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.12 im CIS AWS Foundations Benchmark v1.2 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

> **Note**
>
> Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.
> Die Prüfung führt in den folgenden Fällen zu `FAILED` Ergebnissen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.

2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventName=CreateCustomerGateway) \|\| ($.eventName=DeleteCustomerGateway) || ($.eventName=AttachInternetGateway) \|\| ($.eventName=CreateInternetGateway) || ($.eventName=DeleteInternetGateway) \|\| ($.eventName=DetachInternetGateway)}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Größer/Gleich
als...	**`1`**

[CloudWatch.13] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.13, CIS Foundations Benchmark v1.4.0/4.13 AWS

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

`AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::Trail`Ressourcentyp:,, `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Sie API-Aufrufe in Echtzeit überwachen, indem es CloudTrail CloudWatch Protokolle an Logs weiterleitet und entsprechende Metrikfilter und Alarme einrichtet. Routing-Tabellen leiten Netzwerkdatenverkehr zwischen Subnetzen und Netzwerk-Gateways weiter.

CIS empfiehlt, einen Metrikfilter und einen Alarm für Änderungen an Routing-Tabellen zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass sämtlicher VPC-Datenverkehr durch einen erwarteten Pfad fließt.

> **Note**
>
> Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.
> Die Prüfung führt in den folgenden Fällen zu `FAILED` Ergebnissen:
>
> - Es ist kein Trail konfiguriert.
> - Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.
>
> Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

> **Note**
>
> Unser empfohlenes Filtermuster für diese Behebungsschritte unterscheidet sich von dem Filtermuster in den CIS-Leitlinien. Unsere empfohlenen Filter zielen nur auf Ereignisse ab, die aus API-Aufrufen von Amazon Elastic Compute Cloud (EC2) stammen.

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.

2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.

3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventSource=ec2.amazonaws.com) && (($.eventName=CreateRoute) || ($.eventName=CreateRouteTable) \|\| ($.eventName=ReplaceRoute) || ($.eventName=ReplaceRouteTableAssociation) \|\| ($.eventName=DeleteRouteTable) || ($.eventName=DeleteRoute) \|\| ($.eventName=DisassociateRouteTable))}`
Metrischer Namespace	**`LogMetrics`**
Metrikwert	**`1`**
Standardwert	**`0`**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Größer/Gleich

Feld	Value (Wert)
als...	**1**

[CloudWatch.14] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/3.14, CIS Foundations Benchmark v1.4.0/4.14 AWS

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

`AWS::Logs::MetricFilterAWS::CloudWatch::AlarmAWS::CloudTrail::Trail`Ressourcentyp:,, `AWS::SNS::Topic`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Sie können API-Aufrufe in Echtzeit überwachen, indem Sie CloudTrail Protokolle in Logs umleiten und entsprechende metrische Filter und Alarme einrichten. CloudWatch Sie können mehr als eine VPC in Ihrem Konto haben und eine Peer-Verbindung zwischen zwei VPCs erstellen, sodass Netzwerkdatenverkehr zwischen VPCs weitergeleitet werden kann.

CIS empfiehlt, einen metrischen Filter und einen Alarm für Änderungen an VPCs zu erstellen. Die Überwachung dieser Änderungen hilft sicherzustellen, dass Authentifizierungs- und Autorisierungskontrollen intakt bleiben.

Um diese Prüfung durchzuführen, verwendet Security Hub benutzerdefinierte Logik, um genau die Auditschritte durchzuführen, die für Kontrolle 4.14 im CIS AWS Foundations Benchmark v1.4.0 vorgeschrieben sind. Dieses Steuerelement fällt aus, wenn die von CIS vorgeschriebenen genauen metrischen Filter nicht verwendet werden. Zusätzliche Felder oder Bedingungen können den Metrikfiltern nicht hinzugefügt werden.

Note

Wenn Security Hub die Prüfung für dieses Steuerelement durchführt, sucht es nach CloudTrail Spuren, die das Girokonto verwendet. Bei diesen Trails kann es sich um Organisations-Trails handeln, die zu einem anderen Konto gehören. Wanderwege mit mehreren Regionen können sich auch in einer anderen Region befinden.
Die Prüfung führt in den folgenden Fällen zu `FAILED` Ergebnissen:

- Es ist kein Trail konfiguriert.
- Die verfügbaren Wanderwege, die sich in der aktuellen Region befinden und Eigentum von Girokonten sind, entsprechen nicht den Kontrollanforderungen.

Die Prüfung ergibt in den folgenden Fällen einen Kontrollstatus von`NO_DATA`:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

  Wir empfehlen Organization Trails, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von `NO_DATA` für Kontrollen, die in den Konten von Organisationsmitgliedern bewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Für den Alarm muss das Girokonto entweder das Amazon SNS SNS-Thema besitzen, auf das verwiesen wird, oder es muss telefonisch Zugriff auf das Amazon SNS SNS-Thema erhalten. `ListSubscriptionsByTopic` Andernfalls generiert Security Hub `WARNING` Ergebnisse für die Kontrolle.

Abhilfe

Um diese Kontrolle zu bestehen, gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema, einen AWS CloudTrail Trail, einen metrischen Filter und einen Alarm für den metrischen Filter zu erstellen.

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide. Erstellen Sie ein Thema, das alle CIS-Alarme empfängt, und erstellen Sie mindestens ein Abonnement für das Thema.
2. Erstellen Sie einen CloudTrail Pfad, der für alle gilt AWS-Regionen. Anweisungen finden Sie im AWS CloudTrail Benutzerhandbuch unter Erstellen eines Pfads.

   Notieren Sie sich den Namen der CloudWatch Logs-Protokollgruppe, die Sie dem CloudTrail Trail zuordnen. Im nächsten Schritt erstellen Sie den Metrikfilter für diese Protokollgruppe.
3. Erstellen Sie einen Metrikfilter. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Metrikfilter für eine Protokollgruppe erstellen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Muster definieren, Filtermuster	`{($.eventName=CreateVpc) \|\| ($.eventName=DeleteVpc) || ($.eventName=ModifyVpcAttribute) \|\| ($.eventName=AcceptVpcPeeringConnection) || ($.eventName=CreateVpcPeeringConnection) \|\| ($.eventName=DeleteVpcPeeringConnection) || ($.eventName=RejectVpcPeeringConnection) \|\| ($.eventName=AttachClassicLinkVpc) || ($.eventName=DetachClassicLinkVpc) \|\| ($.eventName=DisableVpcClassicLink) || ($.eventName=EnableVpcClassicLink)}`
Metrischer Namespace	**`LogMetrics`**

Feld	Value (Wert)
Metrikwert	**1**
Standardwert	**0**

4. Erstellen Sie einen Alarm auf der Grundlage des Filters. Anweisungen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen eines CloudWatch Alarms auf der Grundlage eines Metrikfilters für Protokollgruppen. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Bedingungen, Typ des Schwellenwerts	Statisch
Wann immer *`your-metric-name`* ist...	Größer/Gleich
als...	**1**

[CloudWatch.15] Für CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein

Kategorie: Erkennung > Erkennungsservices

Verwandte Anforderungen: NIST.800-53.R5 AU-6 (1), NIST.800-53.R5 AU-6 (5), NIST.800-53.R5 CA-7, NIst.800-53.R5 IR-4 (1), NIST.800-53.R5 IR-4 (5), NIst.800-53.R5 SI-2, NIst.800-53.R5 SI-20, NIst.800-53,R5 SI-4 (12), NIST.800-53,R5 SI-4 (5)

Schweregrad: Hoch

Art der Ressource: `AWS::CloudWatch::Alarm`

AWS Config Regel: **`cloudwatch-alarm-action-check`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`alarmActionRequired`	Die Steuerung ermittelt, `PASSED` ob der Parameter auf eingestellt ist `true` und ob der Alarm eine Aktion ausführt, wenn der Alarmstatus zu wechselt`ALARM`.	Boolesch	Nicht anpassbar	`true`
`insufficientDataActionRequired`	Die Steuerung ermittelt, `PASSED` ob der Parameter auf eingestellt ist `true` und ob der Alarm eine Aktion ausführt, wenn der Alarmstatus zu wechselt`INSUFFICIENT_DATA` .	Boolesch	`true` oder `false`	`false`
`okActionRequired`	Die Steuerung gibt einen `PASSED` Befund aus, wenn der Parameter auf eingestellt ist `true` und der Alarm eine Aktion ausführt, wenn sich der Alarmstatus auf ändert`OK`.	Boolesch	`true` oder `false`	`false`

Dieses Steuerelement prüft, ob für einen CloudWatch Amazon-Alarm mindestens eine Aktion für den `ALARM` Status konfiguriert ist. Die Steuerung schlägt fehl, wenn für den Alarm keine Aktion für den `ALARM` Status konfiguriert ist. Optional können Sie benutzerdefinierte Parameterwerte angeben, sodass auch Alarmaktionen für die `OK` Zustände `INSUFFICIENT_DATA` oder erforderlich sind.

> **Note**
>
> Security Hub bewertet diese Kontrolle auf der Grundlage CloudWatch metrischer Alarme. Metrische Alarme können Teil von zusammengesetzten Alarmen sein, für die die

angegebenen Aktionen konfiguriert sind. Die Steuerung generiert `FAILED` Ergebnisse in den folgenden Fällen:

- Die angegebenen Aktionen sind nicht für einen metrischen Alarm konfiguriert.
- Der metrische Alarm ist Teil eines zusammengesetzten Alarms, für den die angegebenen Aktionen konfiguriert sind.

Diese Steuerung konzentriert sich darauf, ob für einen CloudWatch Alarm eine Alarmaktion konfiguriert ist, wohingegen sich CloudWatch.17 auf den Aktivierungsstatus einer CloudWatch Alarmaktion konzentriert.

Wir empfehlen CloudWatch Alarmaktionen, um Sie automatisch zu benachrichtigen, wenn eine überwachte Metrik den definierten Schwellenwert überschreitet. Mithilfe von Überwachungsalarmen können Sie ungewöhnliche Aktivitäten erkennen und schnell auf Sicherheits- und Betriebsprobleme reagieren, wenn ein Alarm in einen bestimmten Zustand übergeht. Die häufigste Art von Alarmaktion besteht darin, einen oder mehrere Benutzer zu benachrichtigen, indem eine Nachricht an ein Amazon Simple Notification Service (Amazon SNS) -Thema gesendet wird.

Abhilfe

Informationen zu Aktionen, die von CloudWatch Alarmen unterstützt werden, finden Sie unter Alarmaktionen im CloudWatch Amazon-Benutzerhandbuch.

[CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden

Kategorie: Identifizieren > Protokollierung

Verwandte Anforderungen: NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-11, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.r5 SI-12

Schweregrad: Mittel

Art der Ressource: `AWS::Logs::LogGroup`

AWS Config Regel: **`cw-loggroup-retention-period-check`**

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert	
`minRetentionTime`	Mindestaufbewahrungsdauer in Tagen für CloudWatch Protokollgruppen	Enum	`365`, `400`, `545`, `731`, `1827`, `3653`	`365`	

Diese Kontrolle prüft, ob eine CloudWatch Amazon-Protokollgruppe eine Aufbewahrungsfrist von mindestens der angegebenen Anzahl von Tagen hat. Die Kontrolle schlägt fehl, wenn die Aufbewahrungsdauer unter der angegebenen Anzahl liegt. Sofern Sie keinen benutzerdefinierten Parameterwert für den Aufbewahrungszeitraum angeben, verwendet Security Hub einen Standardwert von 365 Tagen.

CloudWatch Protokolle zentralisieren die Protokolle all Ihrer Systeme und Anwendungen AWS-Services in einem einzigen, hoch skalierbaren Service. Sie können CloudWatch Logs verwenden, um Ihre Protokolldateien von Amazon Elastic Compute Cloud (EC2) -Instances, Amazon Route 53 und anderen Quellen zu überwachen AWS CloudTrail, zu speichern und darauf zuzugreifen. Wenn Sie Ihre Protokolle mindestens ein Jahr lang aufbewahren, können Sie die Aufbewahrungsstandards für Protokolle einhalten.

Abhilfe

Informationen zur Konfiguration der Protokollaufbewahrungseinstellungen finden Sie unter Ändern der Aufbewahrung von Protokolldaten in CloudWatch Logs im CloudWatch Amazon-Benutzerhandbuch.

[CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein

Kategorie: Erkennung > Erkennungsservices

Verwandte Anforderungen: NIST.800-53.R5 AU-6 (1), NIST.800-53.R5 AU-6 (5), NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-2, NIst.800-53.R5 SI-4 (12)

Schweregrad: Hoch

Art der Ressource: `AWS::CloudWatch::Alarm`

AWS Config Regel: **`cloudwatch-alarm-action-enabled-check`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob CloudWatch Alarmaktionen aktiviert sind (`ActionEnabled`sollte auf true gesetzt sein). Die Steuerung schlägt fehl, wenn die Alarmaktion für einen CloudWatch Alarm deaktiviert ist.

> **Note**
>
> Security Hub bewertet diese Kontrolle auf der Grundlage CloudWatch metrischer Alarme. Metrische Alarme können Teil von zusammengesetzten Alarmen sein, bei denen die Alarmaktionen aktiviert sind. Die Steuerung generiert `FAILED` Ergebnisse in den folgenden Fällen:
>
> - Die angegebenen Aktionen sind nicht für einen metrischen Alarm konfiguriert.
> - Der metrische Alarm ist Teil eines zusammengesetzten Alarms, für den Alarmaktionen aktiviert sind.

Diese Steuerung konzentriert sich auf den Aktivierungsstatus einer CloudWatch Alarmaktion, wohingegen sich CloudWatch.15 darauf konzentriert, ob eine `ALARM` Aktion in einem CloudWatch Alarm konfiguriert ist.

Alarmaktionen benachrichtigen Sie automatisch, wenn eine überwachte Metrik den definierten Schwellenwert überschreitet. Wenn die Alarmaktion deaktiviert ist, werden keine Aktionen ausgeführt, wenn sich der Status des Alarms ändert, und Sie werden nicht über Änderungen der überwachten Messwerte informiert. Wir empfehlen, CloudWatch Alarmaktionen zu aktivieren, damit Sie schnell auf Sicherheits- und Betriebsprobleme reagieren können.

Abhilfe

Um eine CloudWatch Alarmaktion zu aktivieren (Konsole)

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.

2. Wählen Sie im Navigationsbereich unter Alarme die Option Alle Alarme aus.
3. Wählen Sie den Alarm aus, für den Sie Aktionen aktivieren möchten.
4. Wählen Sie für Aktionen die Option Alarmaktionen — neu und dann Aktivieren aus.

Weitere Informationen zur Aktivierung von CloudWatch Alarmaktionen finden Sie unter Alarmaktionen im CloudWatch Amazon-Benutzerhandbuch.

AWS CodeArtifact Steuerungen

Diese Kontrollen beziehen sich auf CodeArtifact Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::CodeArtifact::Repository`

AWS Config Regel: `tagged-codeartifact-repository` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS CodeArtifact Repository Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn das Repository keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Repository mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem CodeArtifact Repository finden Sie unter Markieren eines Repositorys CodeArtifact im AWS CodeArtifact Benutzerhandbuch.

AWS CodeBuild Steuerungen

Diese Kontrollen beziehen sich auf CodeBuild Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten

Verwandte Anforderungen: PCI DSS v3.2.1/8.2.1, NIST.800-53.R5 SA-3

Kategorie: Schutz > Sichere Entwicklung

Schweregrad: Kritisch

Art der Ressource: `AWS::CodeBuild::Project`

AWS Config -Regel: `codebuild-project-source-repo-url-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die URL AWS CodeBuild des Bitbucket-Quell-Repositorys eines Projekts persönliche Zugriffstoken oder einen Benutzernamen und ein Passwort enthält. Die Kontrolle schlägt fehl, wenn die URL des Bitbucket-Quell-Repositorys persönliche Zugriffstoken oder einen Benutzernamen und ein Passwort enthält.

> **Note**
>
> Dieses Steuerelement bewertet sowohl die Primärquelle als auch die Sekundärquellen eines CodeBuild Build-Projekts. Weitere Informationen zu Projektquellen finden Sie im AWS CodeBuild Benutzerhandbuch unter Beispiel für mehrere Eingabequellen und Ausgabeartefakte.

Anmeldeinformationen sollten nicht im Klartext gespeichert oder übertragen werden oder in der Quell-Repository-URL erscheinen. Statt persönlicher Zugriffstoken oder Anmeldedaten solltest du auf deinen Quellanbieter zugreifen und deine Quell-Repository-URL so ändern CodeBuild, dass sie nur den Pfad zum Bitbucket-Repository-Speicherort enthält. Die Verwendung persönlicher Zugriffstoken oder Anmeldedaten könnte zu unbeabsichtigter Offenlegung von Daten oder unberechtigtem Zugriff führen.

Abhilfe

Sie können Ihr CodeBuild Projekt so aktualisieren, dass es OAuth verwendet.

Um das persönliche Zugriffstoken für die Standardauthentifizierung/(GitHub) aus CodeBuild der Projektquelle zu entfernen

1. Öffnen Sie die CodeBuild Konsole unter https://console.aws.amazon.com/codebuild/.
2. Wählen Sie das Build-Projekt aus, das persönliche Zugriffstoken oder einen Benutzernamen und ein Passwort enthält.
3. Wählen Sie unter Edit (Bearbeiten) die Option Source (Quelle) aus.
4. Wähle Disconnect from GitHub //Bitbucket aus.
5. Wähle Connect using OAuth und dann Connect to GitHub//Bitbucket.
6. Wenn Sie dazu aufgefordert werden, wählen Sie Autorisieren entsprechend aus.
7. Konfigurieren Sie Ihre Repository-URL und zusätzliche Konfigurationseinstellungen nach Bedarf neu.
8. Wählen Sie Update source (Quelle aktualisieren) aus.

Weitere Informationen findest du in den CodeBuild Anwendungsbeispielen im Benutzerhandbuch.AWS CodeBuild

[CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten

Verwandte Anforderungen: PCI DSS v3.2.1/8.2.1, NIST.800-53.R5 IA-5 (7), NIST.800-53.R5 SA-3

Kategorie: Schutz > Sichere Entwicklung

Schweregrad: Kritisch

Art der Ressource: `AWS::CodeBuild::Project`

AWS Config -Regel: `codebuild-project-envvar-awscred-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob das Projekt die Umgebungsvariablen `AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY` enthält.

Die Anmeldeinformationen für die Authentifizierung `AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY` sollten niemals in Klartext gespeichert werden, da dies zu einer unbeabsichtigten Datenoffenlegung und unbefugtem Zugriff führen kann.

Abhilfe

Informationen zum Entfernen von Umgebungsvariablen aus einem CodeBuild Projekt finden Sie AWS CodeBuild im AWS CodeBuild Benutzerhandbuch unter Ändern der Einstellungen eines Build-Projekts. Stellen Sie sicher, dass nichts für Umgebungsvariablen ausgewählt ist.

Sie können Umgebungsvariablen mit sensiblen Werten im AWS Systems Manager Parameterspeicher speichern oder AWS Secrets Manager sie dann aus Ihrer Build-Spezifikation abrufen. Anweisungen finden Sie im AWS CodeBuild Benutzerhandbuch im Feld „Wichtig“ im Abschnitt „Umgebung“.

[CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Niedrig

Art der Ressource: `AWS::CodeBuild::Project`

AWS Config -Regel: `codebuild-project-s3-logs-encrypted`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob Amazon S3 S3-Protokolle für ein AWS CodeBuild Projekt verschlüsselt sind. Die Kontrolle schlägt fehl, wenn die Verschlüsselung für S3-Protokolle für ein CodeBuild Projekt deaktiviert ist.

Die Verschlüsselung von Daten im Ruhezustand ist eine empfohlene bewährte Methode, um Ihre Daten um eine Ebene der Zugriffsverwaltung zu erweitern. Durch die Verschlüsselung der Protokolle

im Ruhezustand AWS wird das Risiko verringert, dass ein Benutzer, der sich nicht authentifiziert hat, auf die auf der Festplatte gespeicherten Daten zugreift. Es fügt weitere Zugriffskontrollen hinzu, um den Zugriff nicht autorisierter Benutzer auf die Daten einzuschränken.

Abhilfe

Informationen zum Ändern der Verschlüsselungseinstellungen für CodeBuild Projekt-S3-Protokolle finden Sie AWS CodeBuild im AWS CodeBuild Benutzerhandbuch unter Ändern der Einstellungen eines Build-Projekts.

[CodeBuild1.4] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (12), NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIst.800-53.R5 AU-10, NIst.800-53.R5 AU-2, NIST.800-53.R5 AU-2 800-53.R5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 AU-9 (7), NIST.800-53.R5 CA-7, NIst.800-53.R5 SC-7 (9), NIst.800-53.R5 SI-3 (8), NIst.800-53.R5 SI-4, NIST.800-53,R5 SI-4 (20), NIST.800-53,R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::CodeBuild::Project`

AWS Config -Regel: `codebuild-project-logging-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine CodeBuild Projektumgebung über mindestens eine Protokolloption verfügt, entweder für S3 oder ob CloudWatch Protokolle aktiviert sind. Dieses Steuerelement schlägt fehl, wenn in einer CodeBuild Projektumgebung nicht mindestens eine Protokolloption aktiviert ist.

Aus Sicherheitsgründen ist die Protokollierung eine wichtige Funktion, um future forensische Maßnahmen im Falle von Sicherheitsvorfällen zu ermöglichen. Die Korrelation von Anomalien in CodeBuild Projekten mit Bedrohungserkennungen kann das Vertrauen in die Genauigkeit dieser Bedrohungserkennungen erhöhen.

Abhilfe

Weitere Informationen zur Konfiguration der CodeBuild Projektprotokolleinstellungen finden Sie im Benutzerhandbuch unter Erstellen eines Build-Projekts (Konsole). CodeBuild

[CodeBuild.5] In CodeBuild Projektumgebungen sollte der privilegierte Modus nicht aktiviert sein

> **Important**
>
> Security Hub hat diese Kontrolle im April 2024 eingestellt. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIst.800-53.R5 AC-5, NIST.800-53.R5 AC-6, NIst.800-53.R5 AC-6 (10), NIst.800-53,5r5 AC-6 (2)

Kategorie: Schützen > Sicheres Zugriffsmanagement

Schweregrad: Hoch

Art der Ressource: `AWS::CodeBuild::Project`

AWS Config -Regel: `codebuild-project-environment-privileged-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einer AWS CodeBuild Projektumgebung der privilegierte Modus aktiviert oder deaktiviert ist. Die Steuerung schlägt fehl, wenn in einer CodeBuild Projektumgebung der privilegierte Modus aktiviert ist.

Standardmäßig erlauben Docker-Container keinen Zugriff auf Geräte. Der privilegierte Modus gewährt dem Docker-Container eines Build-Projekts Zugriff auf alle Geräte. Die Einstellung `privilegedMode` mit einem Wert `true` ermöglicht es dem Docker-Daemon, in einem Docker-Container ausgeführt zu werden. Der Docker-Daemon wartet auf Docker-API-Anfragen und verwaltet Docker-Objekte wie Images, Container, Netzwerke und Volumes. Dieser Parameter sollte nur auf true gesetzt werden, wenn das Build-Projekt zum Erstellen von Docker-Images verwendet wird. Andernfalls sollte diese Einstellung deaktiviert werden, um einen unbeabsichtigten Zugriff auf Docker-

APIs sowie auf die dem Container zugrunde liegende Hardware zu verhindern. Die Einstellung `privilegedMode` auf `false` trägt dazu bei, kritische Ressourcen vor Manipulation und Löschung zu schützen.

Abhilfe

Informationen zum Konfigurieren der Einstellungen für die CodeBuild Projektumgebung finden Sie im CodeBuild Benutzerhandbuch unter Erstellen eines Build-Projekts (Konsole). Wählen Sie im Abschnitt Umgebung nicht die Einstellung Privilegiert aus.

AWS Config steuert

Diese Kontrollen beziehen sich auf AWS Config Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Config.1] AWS Config sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v3.2.1/10.5.2, PCI DSS v3.2.1/11.5, CIS AWS Foundations Benchmark v1.2.0/2.5, CIS Foundations Benchmark v1.4.0/3.5, CIS Foundations Benchmark v3.0.0/3.3, NIST.800-53.R5 AWS CM-3, NIST.800-53.R5 CM-6 (1), NIST.800-53.r5 AWS CM-8, NIST.800-53.r5 CM-8 (2)

Kategorie: Identifizieren > Bestand

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config Regel: Keine (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob sie in Ihrem Konto in der aktuellen Region aktiviert AWS Config ist, und zeichnet alle Ressourcen auf. Die Steuerung schlägt fehl, wenn sie AWS Config nicht aktiviert ist oder nicht alle Ressourcen aufzeichnet.

Der AWS Config Dienst führt die Konfigurationsverwaltung der unterstützten AWS Ressourcen in Ihrem Konto durch und stellt Ihnen Protokolldateien zur Verfügung. Zu den aufgezeichneten

Informationen gehören das Konfigurationselement (AWS Ressource), Beziehungen zwischen Konfigurationselementen und alle Konfigurationsänderungen zwischen Ressourcen.

Security Hub empfiehlt die Aktivierung AWS Config in allen Regionen. Der Verlauf der AWS Konfigurationselemente, der AWS Config aufgezeichnet wird, ermöglicht Sicherheitsanalysen, die Nachverfolgung von Ressourcenänderungen und die Überprüfung der Einhaltung von Vorschriften.

> **Note**
>
> Config.1 setzt voraus, dass dies in allen Regionen aktiviert AWS Config ist, in denen Sie Security Hub verwenden.
> Da es sich bei Security Hub um einen regionalen Dienst handelt, wird bei der für dieses Steuerelement durchgeführten Prüfung nur die aktuelle Region für das Konto geprüft. Es werden nicht alle Regionen überprüft.
> Um Sicherheitsprüfungen für globale Ressourcen in jeder Region zu ermöglichen, müssen Sie auch globale Ressourcen aufzeichnen. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.
> Die weltweit erfassten Ressourcentypen, die AWS Config unterstützt werden, sind IAM-Benutzer, Gruppen, Rollen und vom Kunden verwaltete Richtlinien. Sie können erwägen, Security Hub-Steuerelemente, die diese Ressourcentypen überprüfen, in Regionen zu deaktivieren, in denen die globale Ressourcenaufzeichnung deaktiviert ist. Da es sich bei IAM um einen globalen Dienst handelt, werden IAM-Ressourcen nur in der Region aufgezeichnet, in der die globale Ressourcenaufzeichnung aktiviert ist. Weitere Informationen finden Sie unter Security Hub-Steuerelemente, die Sie möglicherweise deaktivieren möchten.

Abhilfe

Informationen zur Aktivierung AWS Config und Konfiguration für die Aufzeichnung aller Ressourcen finden Sie unter Manuelles Setup im AWS Config Entwicklerhandbuch. Um globale Ressourcen aufzuzeichnen und sicherzustellen, dass keine Ressourcentypen ausgeschlossen werden, wählen Sie Alle Ressourcen mit anpassbaren Überschreibungen aus. Entfernen Sie alle Override-Einstellungen und setzen Sie die Aufnahmefrequenz auf Kontinuierliche Aufnahme.

Sie können diesen Vorgang auch mithilfe einer AWS CloudFormation Vorlage automatisieren. Weitere Informationen finden Sie in den AWS CloudFormation StackSets Beispielvorlagen im AWS CloudFormation Benutzerhandbuch.

Amazon Data Firehose-Steuerelemente

Diese Kontrollen beziehen sich auf Amazon Data Firehose-Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIst.800-53.R5 AC-3, NIST.800-53.R5 AU-3, NIST.800-53.R5 SC-12, NIST.800-53.R5 SC-13, NIst.800-53.R5 SC-28

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::KinesisFirehose::DeliveryStream`

AWS Config -Regel: `kinesis-firehose-delivery-stream-encrypted`

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon Data Firehose-Lieferstream im Ruhezustand mit serverseitiger Verschlüsselung verschlüsselt ist. Diese Steuerung schlägt fehl, wenn ein Firehose-Lieferstream im Ruhezustand nicht mit serverseitiger Verschlüsselung verschlüsselt ist.

Die serverseitige Verschlüsselung ist eine Funktion in Amazon Data Firehose-Lieferströmen, die Daten automatisch verschlüsselt, bevor sie gespeichert werden, indem ein in AWS Key Management Service () erstellter Schlüssel verwendet wird.AWS KMS Daten werden verschlüsselt, bevor sie in die Data Firehose-Stream-Speicherschicht geschrieben werden, und entschlüsselt, nachdem sie aus dem Speicher abgerufen werden. Auf diese Weise können Sie die gesetzlichen Anforderungen erfüllen und die Sicherheit Ihrer Daten verbessern.

Abhilfe

Informationen zur Aktivierung der serverseitigen Verschlüsselung für Firehose-Lieferstreams finden Sie unter Datenschutz in Amazon Data Firehose im Amazon Data Firehose Developer Guide.

Amazon Detective steuert

Diese Kontrollen beziehen sich auf die Ressourcen von Detective.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Detective.1] Verhaltensdiagramme von Detektiven sollten markiert werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::Detective::Graph`

AWS Config Regel: `tagged-detective-graph` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein Amazon Detective-Verhaltensdiagramm Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn das Verhaltensdiagramm keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Verhaltensdiagramm mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck,

Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Verhaltensdiagramm von Detective finden Sie unter Hinzufügen von Tags zu einem Verhaltensdiagramm im Amazon Detective Administration Guide.

AWS Database Migration Service Steuerungen

Diese Kontrollen beziehen sich auf AWS DMS Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.6, NIST.800-53.R5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.R5 AC-3. R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5

SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21)), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: `AWS::DMS::ReplicationInstance`

AWS Config -Regel: `dms-replication-not-public`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob AWS DMS Replikationsinstanzen öffentlich sind. Zu diesem Zweck untersucht es den Wert des `PubliclyAccessible` Felds.

Eine private Replikationsinstanz hat eine private IP-Adresse, auf die Sie außerhalb des Replikationsnetzwerks nicht zugreifen können. Eine Replikationsinstanz sollte eine private IP-Adresse haben, wenn sich die Quell- und Zieldatenbank im selben Netzwerk befinden. Das Netzwerk muss auch über ein VPN oder VPC-Peering mit der VPC der Replikationsinstanz verbunden sein. AWS Direct ConnectWeitere Informationen zu öffentlichen und privaten Replikationsinstanzen finden Sie im Benutzerhandbuch unter Öffentliche und private Replikationsinstanzen.AWS Database Migration Service

Sie sollten außerdem sicherstellen, dass der Zugriff auf Ihre AWS DMS Instanzkonfiguration nur autorisierten Benutzern vorbehalten ist. Beschränken Sie dazu die IAM-Berechtigungen der Benutzer, AWS DMS Einstellungen und Ressourcen zu ändern.

Abhilfe

Sie können die Einstellung für den öffentlichen Zugriff für eine DMS-Replikationsinstanz nicht ändern, nachdem Sie sie erstellt haben. Um die Einstellung für den öffentlichen Zugriff zu ändern, löschen Sie Ihre aktuelle Instanz und erstellen Sie sie anschließend neu. Wählen Sie nicht die Option Öffentlich zugänglich aus.

[DMS.2] DMS-Zertifikate sollten gekennzeichnet sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::DMS::Certificate`

AWS Config Regel: `tagged-dms-certificate` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein AWS DMS Zertifikat Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn das Zertifikat keine Tagschlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Zertifikat mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen

möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem DMS-Zertifikat finden Sie unter Ressourcen kennzeichnen AWS Database Migration Service im Benutzerhandbuch.AWS Database Migration Service

[DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::DMS::EventSubscription`

AWS Config Regel: `tagged-dms-eventsubscription` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList	Liste der Tags, die die AWS	`No default value`

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen	

Dieses Steuerelement prüft, ob ein AWS DMS Ereignisabonnement Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn das Ereignisabonnement keine Tagschlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Ereignisabonnement mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem DMS-Veranstaltungsabonnement finden Sie AWS Database Migration Service im Benutzerhandbuch unter Ressourcen taggen.AWS Database Migration Service

[DMS.4] DMS-Replikationsinstanzen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::DMS::ReplicationInstance`

AWS Config Regel: `tagged-dms-replicationinstance` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob eine AWS DMS Replikationsinstanz über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn die Replikationsinstanz keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl,

wenn die Replikationsinstanz mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer DMS-Replikationsinstanz finden Sie unter Ressourcen taggen AWS Database Migration Service im Benutzerhandbuch.AWS Database Migration Service

[DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::DMS::ReplicationSubnetGroup`

AWS Config Regel: `tagged-dms-replicationsubnetgroup` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob eine AWS DMS Replikationssubnetzgruppe Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Replikationssubnetzgruppe keine Tagschlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Replikationssubnetzgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer DMS-Replikationssubnetzgruppe finden Sie unter Ressourcen kennzeichnen im AWS Database Migration Service Benutzerhandbuch.AWS Database Migration Service

[DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5)

Kategorie: Erkennen > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::DMS::ReplicationInstance`

AWS Config -Regel: `dms-auto-minor-version-upgrade-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob das automatische Upgrade einer Nebenversion für eine AWS DMS Replikationsinstanz aktiviert ist. Die Steuerung schlägt fehl, wenn das automatische Upgrade der Nebenversion für eine DMS-Replikationsinstanz nicht aktiviert ist.

DMS bietet ein automatisches Upgrade der Nebenversionen für jede unterstützte Replikationsengine, sodass Sie Ihre Replikationsinstanz behalten können. up-to-date Nebenversionen können neue Softwarefunktionen, Bugfixes, Sicherheitspatches und Leistungsverbesserungen einführen. Durch die Aktivierung der automatischen Aktualisierung kleinerer Versionen auf DMS-Replikationsinstanzen

werden kleinere Upgrades automatisch während des Wartungsfensters oder sofort angewendet, wenn die Option Änderungen sofort anwenden ausgewählt ist.

Abhilfe

Informationen zur Aktivierung des automatischen Upgrades für Nebenversionen auf DMS-Replikationsinstanzen finden Sie unter Ändern einer Replikationsinstanz im AWS Database Migration Service Benutzerhandbuch.

[DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.r5 AU-3 R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::DMS::ReplicationTask`

AWS Config -Regel: `dms-replication-task-targetdb-logging`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung mit dem Mindestschweregrad `LOGGER_SEVERITY_DEFAULT` für DMS-Replikationsaufgaben `TARGET_APPLY` und `TARGET_LOAD` aktiviert ist. Die Steuerung schlägt fehl, wenn die Protokollierung für diese Aufgaben nicht aktiviert ist oder wenn der Mindestschweregrad unter `LOGGER_SEVERITY_DEFAULT` liegt.

DMS verwendet Amazon CloudWatch , um Informationen während des Migrationsprozesses zu protokollieren. Mithilfe der Einstellungen für die Protokollierungsaufgabe können Sie angeben, welche Komponentenaktivitäten protokolliert werden und wie viele Informationen protokolliert werden. Sie sollten die Protokollierung für die folgenden Aufgaben angeben:

- `TARGET_APPLY` – Daten und Data Definition Language (DDL)-Anweisungen werden auf die Zieldatenbank angewendet.

- `TARGET_LOAD` – Daten werden in die Zieldatenbank geladen.

Die Protokollierung spielt bei DMS-Replikationsaufgaben eine entscheidende Rolle, da sie Überwachung, Problembehandlung, Prüfung, Leistungsanalyse, Fehlererkennung und Wiederherstellung sowie historische Analysen und Berichte ermöglicht. Es trägt dazu bei, die erfolgreiche Replikation von Daten zwischen Datenbanken sicherzustellen und gleichzeitig die Datenintegrität und die Einhaltung gesetzlicher Anforderungen zu gewährleisten. Andere Protokollierungsstufen als `DEFAULT` werden für diese Komponenten bei der Problembehandlung selten benötigt. Wir empfehlen, die Protokollierungsebene `DEFAULT` für diese Komponenten beizubehalten, es sei denn, Sie werden ausdrücklich aufgefordert, sie zu ändern AWS Support. Eine minimale Protokollierungsebene von `DEFAULT` stellt sicher, dass Informationsmeldungen, Warnungen und Fehlermeldungen in die Protokolle geschrieben werden. Dieses Steuerelement überprüft, ob die Protokollierungsebene für die vorangegangenen Replikationsaufgaben mindestens einer der folgenden Werte entspricht: `LOGGER_SEVERITY_DEFAULTLOGGER_SEVERITY_DEBUG`, oder`LOGGER_SEVERITY_DETAILED_DEBUG`.

Abhilfe

Informationen zum Aktivieren der Protokollierung für DMS-Replikationsaufgaben in der Zieldatenbank finden Sie unter AWS DMS Task-Logs anzeigen und verwalten im AWS Database Migration Service Benutzerhandbuch.

[DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.r5 AU-3 R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::DMS::ReplicationTask`

AWS Config -Regel: `dms-replication-task-sourcedb-logging`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung mit dem Mindestschweregrad `LOGGER_SEVERITY_DEFAULT` für DMS-Replikationsaufgaben `SOURCE_CAPTURE` und `SOURCE_UNLOAD` aktiviert ist. Die Steuerung schlägt fehl, wenn die Protokollierung für diese Aufgaben nicht aktiviert ist oder wenn der Mindestschweregrad unter `LOGGER_SEVERITY_DEFAULT` liegt.

DMS verwendet Amazon CloudWatch , um Informationen während des Migrationsprozesses zu protokollieren. Mithilfe der Einstellungen für die Protokollierungsaufgabe können Sie angeben, welche Komponentenaktivitäten protokolliert werden und wie viele Informationen protokolliert werden. Sie sollten die Protokollierung für die folgenden Aufgaben angeben:

- `SOURCE_CAPTURE`— Laufende Replikations- oder CDC-Daten (Change Data Capture) werden aus der Quelldatenbank oder dem Quelldienst erfasst und an die `SORTER` Servicekomponente weitergegeben.
- `SOURCE_UNLOAD`— Daten werden bei Volllast aus der Quelldatenbank oder dem Quelldienst entladen.

Die Protokollierung spielt bei DMS-Replikationsaufgaben eine entscheidende Rolle, da sie Überwachung, Fehlerbehebung, Prüfung, Leistungsanalyse, Fehlererkennung und Wiederherstellung sowie historische Analysen und Berichte ermöglicht. Es trägt dazu bei, die erfolgreiche Replikation von Daten zwischen Datenbanken sicherzustellen und gleichzeitig die Datenintegrität und die Einhaltung gesetzlicher Anforderungen zu gewährleisten. Andere Protokollierungsstufen als `DEFAULT` werden für diese Komponenten bei der Problembehandlung selten benötigt. Wir empfehlen, die Protokollierungsebene `DEFAULT` für diese Komponenten beizubehalten, es sei denn, Sie werden ausdrücklich aufgefordert, sie zu ändern AWS Support. Eine minimale Protokollierungsebene von `DEFAULT` stellt sicher, dass Informationsmeldungen, Warnungen und Fehlermeldungen in die Protokolle geschrieben werden. Dieses Steuerelement überprüft, ob die Protokollierungsebene für die vorangegangenen Replikationsaufgaben mindestens einer der folgenden Werte entspricht: `LOGGER_SEVERITY_DEFAULTLOGGER_SEVERITY_DEBUG`, oder`LOGGER_SEVERITY_DETAILED_DEBUG`.

Abhilfe

Informationen zum Aktivieren der Protokollierung für DMS-Replikationsaufgaben in der Quelldatenbank finden Sie unter AWS DMS Task-Logs anzeigen und verwalten im AWS Database Migration Service Benutzerhandbuch.

[DMS.9] DMS-Endpunkte sollten SSL verwenden

Verwandte Anforderungen: NIst.800-53.R5 AC-4, NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-23, NIST.800-53.R5 SC-23 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIst.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 R5 SC-8 (2)

Kategorie: Schützen > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: `AWS::DMS::Endpoint`

AWS Config -Regel: `dms-endpoint-ssl-configured`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS DMS Endpunkt eine SSL-Verbindung verwendet. Die Steuerung schlägt fehl, wenn der Endpunkt kein SSL verwendet.

SSL/TLS-Verbindungen bieten eine Sicherheitsebene, indem sie Verbindungen zwischen DMS-Replikationsinstanzen und Ihrer Datenbank verschlüsseln. Die Verwendung von Zertifikaten bietet eine zusätzliche Sicherheitsebene, indem überprüft wird, ob die Verbindung zur erwarteten Datenbank hergestellt wird. Dazu wird das Serverzertifikat überprüft, das automatisch auf allen von Ihnen bereitgestellten Datenbankinstanzen installiert wird. Durch die Aktivierung der SSL-Verbindung auf Ihren DMS-Endpunkten schützen Sie die Vertraulichkeit der Daten während der Migration.

Abhilfe

Informationen zum Hinzufügen einer SSL-Verbindung zu einem neuen oder vorhandenen DMS-Endpunkt finden Sie unter SSL verwenden mit AWS Database Migration Service im AWS Database Migration Service Benutzerhandbuch.

[DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-6, NIST.800-53.R5 AC-17, NIST.800-53.R5 IA-2, NIST.800-53.r5 IA-5

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: `AWS::DMS::Endpoint`

AWS Config -Regel: `dms-neptune-iam-authorization-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS DMS Endpunkt für eine Amazon Neptune Neptune-Datenbank mit IAM-Autorisierung konfiguriert ist. Die Kontrolle schlägt fehl, wenn für den DMS-Endpunkt keine IAM-Autorisierung aktiviert ist.

AWS Identity and Access Management (IAM) bietet eine differenzierte Zugriffskontrolle für alle Bereiche. AWS Mit IAM können Sie festlegen, wer unter welchen Bedingungen auf welche Dienste und Ressourcen zugreifen kann. Mit IAM-Richtlinien verwalten Sie die Berechtigungen für Ihre Mitarbeiter und Systeme, um sicherzustellen, dass die Berechtigungen mit den geringsten Rechten eingehalten werden. Indem Sie die IAM-Autorisierung auf AWS DMS Endpunkten für Neptune-Datenbanken aktivieren, können Sie IAM-Benutzern Autorisierungsprivilegien gewähren, indem Sie eine durch den Parameter angegebene Servicerolle verwenden. `ServiceAccessRoleARN`

Abhilfe

Informationen zur Aktivierung der IAM-Autorisierung auf DMS-Endpunkten für Neptune-Datenbanken finden Sie unter Verwenden von Amazon Neptune als Ziel für im Benutzerhandbuch. AWS Database Migration ServiceAWS Database Migration Service

[DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-6, NIST.800-53.R5 IA-2, NIST.800-53.R5 IA-5

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: `AWS::DMS::Endpoint`

AWS Config -Regel: `dms-mongo-db-authentication-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS DMS Endpunkt für MongoDB mit einem Authentifizierungsmechanismus konfiguriert ist. Die Steuerung schlägt fehl, wenn kein Authentifizierungstyp für den Endpunkt festgelegt ist.

AWS Database Migration Service unterstützt zwei Authentifizierungsmethoden für MongoDB — MONGODB-CR für MongoDB Version 2.x und SCRAM-SHA-1 für MongoDB Version 3.x oder höher. Diese Authentifizierungsmethoden werden verwendet, um MongoDB-Passwörter zu authentifizieren und zu verschlüsseln, wenn Benutzer die Passwörter für den Zugriff auf die Datenbanken verwenden möchten. Durch die Authentifizierung auf AWS DMS Endpunkten wird sichergestellt, dass nur autorisierte Benutzer auf die Daten zugreifen und diese ändern können, die zwischen Datenbanken migriert werden. Ohne ordnungsgemäße Authentifizierung können unbefugte Benutzer während des Migrationsprozesses möglicherweise auf sensible Daten zugreifen. Dies kann zu Datenschutzverletzungen, Datenverlust oder anderen Sicherheitsvorfällen führen.

Abhilfe

Informationen zur Aktivierung eines Authentifizierungsmechanismus auf DMS-Endpunkten für MongoDB finden Sie unter Verwenden von MongoDB als Quelle für AWS DMS im Benutzerhandbuch.AWS Database Migration Service

[DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-13

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten währen der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::DMS::Endpoint`

AWS Config -Regel: `dms-redis-tls-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS DMS Endpunkt für Redis mit einer TLS-Verbindung konfiguriert ist. Die Steuerung schlägt fehl, wenn auf dem Endpunkt TLS nicht aktiviert ist.

TLS bietet end-to-end Sicherheit, wenn Daten zwischen Anwendungen oder Datenbanken über das Internet gesendet werden. Wenn Sie die SSL-Verschlüsselung für Ihren DMS-Endpunkt konfigurieren, ermöglicht sie die verschlüsselte Kommunikation zwischen der Quell- und der

Zieldatenbank während des Migrationsprozesses. Dies trägt dazu bei, das Abhören und Abfangen sensibler Daten durch böswillige Akteure zu verhindern. Ohne SSL-Verschlüsselung kann auf sensible Daten zugegriffen werden, was zu Datenschutzverletzungen, Datenverlust oder anderen Sicherheitsvorfällen führen kann.

Abhilfe

Informationen zum Aktivieren einer TLS-Verbindung auf DMS-Endpunkten für Redis finden Sie unter Verwenden von Redis als Ziel für AWS Database Migration Service im Benutzerhandbuch.AWS Database Migration Service

Amazon DocumentDB-Steuerelemente

Diese Steuerelemente beziehen sich auf Amazon DocumentDB DocumentDB-Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `docdb-cluster-encrypted`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon DocumentDB-Cluster im Ruhezustand verschlüsselt ist. Die Kontrolle schlägt fehl, wenn ein Amazon DocumentDB-Cluster im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf alle Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch Verschlüsselung können Sie die

Vertraulichkeit solcher Daten schützen und so das Risiko verringern, dass ein nicht autorisierter Benutzer darauf zugreifen kann. Daten in Amazon DocumentDB-Clustern sollten im Ruhezustand verschlüsselt werden, um eine zusätzliche Sicherheitsebene zu gewährleisten. Amazon DocumentDB verwendet den 256-Bit-Advanced Encryption Standard (AES-256), um Ihre Daten mit den in () gespeicherten Verschlüsselungsschlüsseln zu verschlüsseln. AWS Key Management Service AWS KMS

Abhilfe

Sie können die Verschlüsselung im Ruhezustand aktivieren, wenn Sie einen Amazon DocumentDB-Cluster erstellen. Sie können die Verschlüsselungseinstellungen nach dem Erstellen eines Clusters nicht ändern. Weitere Informationen finden Sie unter Enabling at rest encryption for a Amazon DocumentDB cluster im Amazon DocumentDB Developer Guide.

[DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen

Verwandte Anforderungen: NIST.800-53.R5 SI-12

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: `AWS::RDS::DBCluster`

AWS Config -Regel: `docdb-cluster-backup-retention-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert	
`minimumBackupReten`	Minimale Aufbewahrungsdauer für Backups in Tagen	Ganzzahl	7 auf 35	7	

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert	
`tionPeriod`					

Diese Kontrolle prüft, ob ein Amazon DocumentDB-Cluster eine Aufbewahrungsdauer für Backups hat, die größer oder gleich dem angegebenen Zeitraum ist. Die Kontrolle schlägt fehl, wenn die Aufbewahrungsfrist für Backups den angegebenen Zeitraum unterschreitet. Sofern Sie keinen benutzerdefinierten Parameterwert für die Aufbewahrungsdauer von Backups angeben, verwendet Security Hub einen Standardwert von 7 Tagen.

Backups helfen Ihnen, sich nach einem Sicherheitsvorfall schneller zu erholen und die Widerstandsfähigkeit Ihrer Systeme zu stärken. Durch die Automatisierung von Backups für Ihre Amazon DocumentDB-Cluster können Sie Ihre Systeme zu einem bestimmten Zeitpunkt wiederherstellen und Ausfallzeiten und Datenverluste minimieren. In Amazon DocumentDB haben Cluster eine standardmäßige Aufbewahrungsfrist für Backups von einem Tag. Dieser Wert muss auf einen Wert zwischen 7 und 35 Tagen erhöht werden, um diese Kontrolle zu bestehen.

Abhilfe

Informationen zum Ändern der Aufbewahrungsdauer von Backups für Ihre Amazon DocumentDB-Cluster finden Sie unter Ändern eines Amazon DocumentDB-Clusters im Amazon DocumentDB DocumentDB-Entwicklerhandbuch. Wählen Sie für Backup den Aufbewahrungszeitraum für Backups aus.

[DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein

Verwandte Anforderungen: NIST.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Ressourcentyp:`AWS::RDS::DBClusterSnapshot`, `AWS::RDS:DBSnapshot`

AWS Config -Regel: `docdb-cluster-snapshot-public-prohibited`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein manueller Amazon DocumentDB-Cluster-Snapshot öffentlich ist. Die Kontrolle schlägt fehl, wenn der manuelle Cluster-Snapshot öffentlich ist.

Ein manueller Amazon DocumentDB-Cluster-Snapshot sollte nicht öffentlich sein, es sei denn, dies ist beabsichtigt. Wenn Sie einen unverschlüsselten manuellen Snapshot als öffentlich freigeben, ist der Snapshot für alle verfügbar. AWS-KontenÖffentliche Schnappschüsse können zu einer unbeabsichtigten Offenlegung von Daten führen.

> **Note**
>
> Dieses Steuerelement wertet manuelle Cluster-Snapshots aus. Sie können keinen automatisierten Amazon DocumentDB-Cluster-Snapshot teilen. Sie können jedoch einen manuellen Snapshot erstellen, indem Sie den automatisierten Snapshot kopieren und die Kopie dann teilen.

Abhilfe

Informationen zum Entfernen des öffentlichen Zugriffs für manuelle Cluster-Snapshots von Amazon DocumentDB finden Sie unter Einen Snapshot teilen im Amazon DocumentDB DocumentDB-Entwicklerhandbuch. Programmgesteuert können Sie den Amazon DocumentDB DocumentDB-Vorgang verwenden. `modify-db-snapshot-attribute` Stellen Sie `attribute-name` als und als ein. `restore` `values-to-remove` `all`

[DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.r5

AU-3 R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `docdb-cluster-audit-logging-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon DocumentDB-Cluster Audit-Logs in Amazon CloudWatch Logs veröffentlicht. Die Kontrolle schlägt fehl, wenn der Cluster keine Audit-Logs in Logs veröffentlicht. CloudWatch

Amazon DocumentDB (mit MongoDB-Kompatibilität) ermöglicht es Ihnen, Ereignisse zu überprüfen, die in Ihrem Cluster durchgeführt wurden. Beispiele für protokollierte Ereignisse sind erfolgreiche und fehlgeschlagene Authentifizierungsversuche, Drop-Ereignisse für Sammlungen in einer Datenbank oder das Erstellen eines Index. Standardmäßig ist die Prüfung in Amazon DocumentDB deaktiviert und erfordert, dass Sie Maßnahmen ergreifen, um sie zu aktivieren.

Abhilfe

Informationen zum Veröffentlichen von Amazon DocumentDB-Prüfprotokollen in CloudWatch Logs finden Sie unter Enabling Auditing im Amazon DocumentDB Developer Guide.

[DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2), NIST.800-53.R5 CM-3, NIST.800-53.R5 SC-5 (2)

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `docdb-cluster-deletion-protection-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem Amazon DocumentDB-Cluster der Löschschutz aktiviert ist. Die Kontrolle schlägt fehl, wenn für den Cluster kein Löschschutz aktiviert ist.

Die Aktivierung des Cluster-Löschschutzes bietet einen zusätzlichen Schutz vor versehentlichem Löschen von Datenbanken oder vor dem Löschen durch einen nicht autorisierten Benutzer. Ein Amazon DocumentDB-Cluster kann nicht gelöscht werden, solange der Löschschutz aktiviert ist. Sie müssen zuerst den Löschschutz deaktivieren, bevor eine Löschanfrage erfolgreich sein kann. Der Löschschutz ist standardmäßig aktiviert, wenn Sie einen Cluster in der Amazon DocumentDB DocumentDB-Konsole erstellen.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für einen vorhandenen Amazon DocumentDB-Cluster finden Sie unter Ändern eines Amazon DocumentDB-Clusters im Amazon DocumentDB DocumentDB-Entwicklerhandbuch. Wählen Sie im Abschnitt „Cluster modifizieren“ die Option „Für den Löschschutz aktivieren“.

Amazon DynamoDB-Steuerelemente

Diese Steuerelemente beziehen sich auf DynamoDB-Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[DynamoDB.1] DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-2 (2), NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::DynamoDB::Table`

AWS Config -Regel: `dynamodb-autoscaling-enabled`

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Gültige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`minProvisionedReadCapacity`	Mindestanzahl bereitgestellter Lesekapazitätseinheiten für DynamoDB Auto Scaling	Ganzzahl	1 auf `40000`	Kein Standardwert
`targetReadUtilization`	Zielauslastung in Prozent für die Lesekapazität	Ganzzahl	`20` auf `90`	Kein Standardwert
`minProvisionedWriteCapacity`	Mindestanzahl bereitgestellter Schreibkapazitätseinheiten für DynamoDB Auto Scaling	Ganzzahl	1 auf `40000`	Kein Standardwert
`targetWriteUtilization`	Zielauslastung in Prozent für die Schreibkapazität	Ganzzahl	`20` auf `90`	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon DynamoDB-Tabelle ihre Lese- und Schreibkapazität nach Bedarf skalieren kann. Die Steuerung schlägt fehl, wenn die Tabelle nicht den On-Demand-Kapazitätsmodus oder den Bereitstellungsmodus mit konfigurierter Autoskalierung verwendet. Standardmäßig erfordert dieses Steuerelement nur, dass einer dieser Modi konfiguriert ist, unabhängig von bestimmten Lese- oder Schreibkapazitätsstufen. Optional können Sie benutzerdefinierte Parameterwerte angeben, um bestimmte Lese- und Schreibkapazitäten oder eine bestimmte Zielauslastung zu erfordern.

Durch die bedarfsgerechte Skalierung der Kapazität werden Drosselungen von Ausnahmen vermieden, wodurch die Verfügbarkeit Ihrer Anwendungen aufrechterhalten wird. DynamoDB-Tabellen im On-Demand-Kapazitätsmodus sind nur durch die standardmäßigen Tabellenkontingente für den DynamoDB-Durchsatz begrenzt. Um diese Kontingente zu erhöhen, können Sie ein

Supportticket mit AWS Support.dynamoDB-Tabellen im Bereitstellungsmodus mit auto Skalierung einreichen und die bereitgestellte Durchsatzkapazität dynamisch an Verkehrsmuster anpassen. Weitere Informationen zur DynamoDB-Anforderungsdrosselung finden Sie unter Request Throttling and Burst Capacity im Amazon DynamoDB Developer Guide.

Abhilfe

Informationen zur Aktivierung der automatischen DynamoDB-Skalierung für bestehende Tabellen im Kapazitätsmodus finden Sie unter Aktivieren der auto Skalierung von DynamoDB für bestehende Tabellen im Amazon DynamoDB DynamoDB-Entwicklerhandbuch.

[DynamoDB.2] Bei DynamoDB-Tabellen sollte die Wiederherstellung aktiviert sein point-in-time

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 CP-9, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: `AWS::DynamoDB::Table`

AWS Config -Regel: `dynamodb-pitr-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob point-in-time Recovery (PITR) für eine Amazon DynamoDB-Tabelle aktiviert ist.

Mithilfe von Backups können Sie sich nach einem Sicherheitsvorfall schneller erholen. Sie stärken auch die Widerstandsfähigkeit Ihrer Systeme. Die point-in-time DynamoDB-Wiederherstellung automatisiert Backups für DynamoDB-Tabellen. Es reduziert die Zeit für die Wiederherstellung nach versehentlichen Lösch- oder Schreibvorgängen. DynamoDB-Tabellen, für die PITR aktiviert ist, können zu einem beliebigen Zeitpunkt der letzten 35 Tage wiederhergestellt werden.

Abhilfe

Informationen zum Wiederherstellen einer DynamoDB-Tabelle auf einen bestimmten Zeitpunkt finden Sie unter Wiederherstellen einer DynamoDB-Tabelle auf einen bestimmten Zeitpunkt im Amazon DynamoDB DynamoDB-Entwicklerhandbuch.

[DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6))

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::DynamoDB::Cluster`

AWS Config -Regel: `dax-encryption-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein DAX-Cluster im Ruhezustand verschlüsselt ist.

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass auf Daten, die auf der Festplatte gespeichert sind, von einem Benutzer zugegriffen wird, für den kein Benutzer authentifiziert ist. AWS Durch die Verschlüsselung werden weitere Zugriffskontrollen hinzugefügt, um den Zugriff nicht autorisierter Benutzer auf die Daten zu beschränken. Beispielsweise sind API-Berechtigungen erforderlich, um die Daten zu entschlüsseln, bevor sie gelesen werden können.

Abhilfe

Sie können die Verschlüsselung im Ruhezustand nicht aktivieren oder deaktivieren, nachdem ein Cluster erstellt wurde. Sie müssen den Cluster neu erstellen, um die Verschlüsselung im Ruhezustand zu aktivieren. Ausführliche Anweisungen zum Erstellen eines DAX-Clusters mit aktivierter Verschlüsselung im Ruhezustand finden Sie unter Enabling at rest using the AWS Management Console im Amazon DynamoDB Developer Guide.

[DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6, NIST.800-53.R5 CP-6 (1), NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 CP-9, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellen > Resilienz > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: `AWS::DynamoDB::Table`

AWS Config Regel: **`dynamodb-resources-protected-by-backup-plan`**

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`backupVaultLockCheck`	Das Steuerelement ermittelt, `PASSED` ob der Parameter auf gesetzt ist `true` und die Ressource AWS Backup Vault Lock verwendet.	Boolesch	`true` oder `false`	Kein Standardwert

Dieses Steuerelement bewertet, ob eine Amazon DynamoDB-Tabelle im `ACTIVE` Status durch einen Backup-Plan abgedeckt ist. Die Steuerung schlägt fehl, wenn die DynamoDB-Tabelle nicht durch einen Backup-Plan abgedeckt ist. Wenn Sie den `backupVaultLockCheck` Parameter auf gleich setzen`true`, wird die Steuerung nur erfolgreich ausgeführt, wenn die DynamoDB-Tabelle in einem AWS Backup gesperrten Tresor gesichert ist.

AWS Backup ist ein vollständig verwalteter Backup-Service, der Ihnen hilft, die Sicherung von Daten auf allen Ebenen zu zentralisieren und zu automatisieren. AWS-Services Mit AWS Backup können Sie Backup-Pläne erstellen, die Ihre Backup-Anforderungen definieren, z. B. wie oft Ihre Daten gesichert werden sollen und wie lange diese Backups aufbewahrt werden sollen. Wenn Sie DynamoDB-Tabellen in Ihre Backup-Pläne aufnehmen, können Sie Ihre Daten vor unbeabsichtigtem Verlust oder Löschung schützen.

Abhilfe

Informationen zum Hinzufügen einer DynamoDB-Tabelle zu einem AWS Backup Backup-Plan finden Sie unter Zuweisen von Ressourcen zu einem Backup-Plan im AWS Backup Entwicklerhandbuch.

[DynamoDB.5] DynamoDB-Tabellen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::DynamoDB::Table`

AWS Config Regel: `tagged-dynamodb-table` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob eine Amazon DynamoDB-Tabelle Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind. `requiredTagKeys` Das Steuerelement schlägt fehl, wenn die Tabelle keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Tabelle mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie

außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer DynamoDB-Tabelle finden Sie unter Tagging resources in DynamoDB im Amazon DynamoDB Developer Guide.

[DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2), NIST.800-53.R5 CM-3, NIST.800-53.R5 SC-5 (2)

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Mittel

Art der Ressource: `AWS::DynamoDB::Table`

AWS Config Regel: **`dynamodb-table-deletion-protection-enabled`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Amazon DynamoDB-Tabelle der Löschschutz aktiviert ist. Das Steuerelement schlägt fehl, wenn für eine DynamoDB-Tabelle kein Löschschutz aktiviert ist.

Mit der Eigenschaft Löschschutz können Sie eine DynamoDB-Tabelle vor versehentlichem Löschen schützen. Durch die Aktivierung dieser Eigenschaft für Tabellen wird sichergestellt, dass Tabellen nicht versehentlich während der regulären Tabellenverwaltung durch Ihre Administratoren gelöscht werden. Dies trägt dazu bei, Störungen Ihres normalen Geschäftsbetriebs zu vermeiden.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für eine DynamoDB-Tabelle finden Sie unter Verwenden des Löschschutzes im Amazon DynamoDB DynamoDB-Entwicklerhandbuch.

[DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.R5 AC-17, NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-23

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten währen der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::DynamoDB::Table`

AWS Config Regel: **`dax-tls-endpoint-encryption`**

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon DynamoDB Accelerator (DAX) -Cluster während der Übertragung verschlüsselt ist, wobei der Endpunktverschlüsselungstyp auf TLS festgelegt ist. Die Steuerung schlägt fehl, wenn der DAX-Cluster bei der Übertragung nicht verschlüsselt wird.

HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer person-in-the-middle oder ähnliche Angriffe verwenden, um den Netzwerkverkehr zu belauschen oder zu manipulieren. Sie sollten nur verschlüsselte Verbindungen über TLS für den Zugriff auf DAX-Cluster zulassen. Die Verschlüsselung von Daten während der Übertragung kann jedoch die Leistung beeinträchtigen. Sie sollten Ihre Anwendung mit aktivierter Verschlüsselung testen, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen.

Abhilfe

Sie können die TLS-Verschlüsselungseinstellung nicht ändern, nachdem Sie einen DAX-Cluster erstellt haben. Um einen vorhandenen DAX-Cluster zu verschlüsseln, erstellen Sie einen neuen

Cluster mit aktivierter Verschlüsselung bei der Übertragung, verlagern Sie den Datenverkehr Ihrer Anwendung darauf und löschen Sie dann den alten Cluster. Weitere Informationen finden Sie unter Verwenden des Löschschutzes im Amazon DynamoDB DynamoDB-Entwicklerhandbuch.

Kontrollen in der Amazon Elastic Container Registry

Diese Kontrollen beziehen sich auf Amazon ECR-Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein

Verwandte Anforderungen: NIST.800-53.R5 RA-5

Kategorie: Identifizieren > Schwachstellen-, Patch- und Versionsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::ECR::Repository`

AWS Config -Regel: `ecr-private-image-scanning-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob für ein privates Amazon ECR-Repository das Scannen von Bildern konfiguriert ist. Die Steuerung schlägt fehl, wenn das private ECR-Repository nicht für Scan on Push oder kontinuierliches Scannen konfiguriert ist.

Das Scannen von ECR-Bildern hilft bei der Identifizierung von Softwareschwachstellen in Ihren Container-Images. Die Konfiguration von Bildscans in ECR-Repositorys bietet eine zusätzliche Überprüfungsebene für die Integrität und Sicherheit der gespeicherten Bilder.

Abhilfe

Informationen zum Konfigurieren von Bildscans für ein ECR-Repository finden Sie unter Scannen von Bildern im Amazon Elastic Container Registry User Guide.

[ECR.2] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.r5 CM-8 (1)

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Mittel

Art der Ressource: `AWS::ECR::Repository`

AWS Config -Regel: `ecr-private-tag-immutability-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem privaten ECR-Repository die Tag-Unveränderlichkeit aktiviert ist. Diese Kontrolle schlägt fehl, wenn in einem privaten ECR-Repository die Tag-Unveränderlichkeit deaktiviert ist. Diese Regel gilt, wenn die Tag-Unveränderlichkeit aktiviert ist und den Wert hat. `IMMUTABLE`

Amazon ECR Tag Immutability ermöglicht es Kunden, sich auf die beschreibenden Tags eines Bildes als zuverlässigen Mechanismus zur Nachverfolgung und eindeutigen Identifizierung von Bildern zu verlassen. Ein unveränderliches Tag ist statisch, was bedeutet, dass sich jedes Tag auf ein eindeutiges Bild bezieht. Dies verbessert die Zuverlässigkeit und Skalierbarkeit, da die Verwendung eines statischen Tags immer dazu führt, dass dasselbe Image bereitgestellt wird. Wenn sie konfiguriert ist, verhindert die Unveränderlichkeit von Tags, dass die Tags überschrieben werden, wodurch die Angriffsfläche reduziert wird.

Abhilfe

Informationen zum Erstellen eines Repositorys mit konfigurierten unveränderlichen Tags oder zum Aktualisieren der Image-Tag-Mutabilitätseinstellungen für ein vorhandenes Repository finden Sie unter Image-Tag-Mutability im Amazon Elastic Container Registry User Guide.

[ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::ECR::Repository`

AWS Config -Regel: `ecr-private-lifecycle-policy-configured`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob für ein Amazon ECR-Repository mindestens eine Lebenszyklusrichtlinie konfiguriert ist. Diese Kontrolle schlägt fehl, wenn für ein ECR-Repository keine Lebenszyklusrichtlinien konfiguriert sind.

Mit Amazon ECR-Lebenszyklusrichtlinien können Sie das Lebenszyklusmanagement von Images in einem Repository festlegen. Durch die Konfiguration von Lebenszyklusrichtlinien können Sie die Bereinigung ungenutzter Images und das Verfallsdatum von Images je nach Alter oder Anzahl automatisieren. Durch die Automatisierung dieser Aufgaben können Sie verhindern, dass versehentlich veraltete Bilder in Ihrem Repository verwendet werden.

Abhilfe

Informationen zur Konfiguration einer Lifecycle-Richtlinie finden Sie unter Creating a Lifecycle Policy Preview im Amazon Elastic Container Registry User Guide.

[ECR.4] Öffentliche ECR-Repositorien sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::ECR::PublicRepository`

AWS Config Regel: `tagged-ecr-publicrepository` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein öffentliches Amazon ECR-Repository Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Kontrolle schlägt fehl, wenn das öffentliche Repository keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das öffentliche Repository mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem öffentlichen ECR-Repository finden Sie unter Tagging an ein öffentliches Amazon ECR-Repository im Amazon Elastic Container Registry-Benutzerhandbuch.

Amazon ECS-Steuerelemente

Diese Kontrollen beziehen sich auf Amazon ECS-Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-5, NIST.800-53.R5 AC-6

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Hoch

Ressourcentyp: `AWS::ECS::TaskDefinition`

AWS Config -Regel: `ecs-task-definition-user-for-host-mode-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `SkipInactiveTaskDefinitions`: `true` (nicht anpassbar)

Dieses Steuerelement prüft, ob eine aktive Amazon ECS-Aufgabendefinition mit Host-Netzwerkmodus `user` Container-Definitionen hat`privileged`. Die Steuerung schlägt bei Aufgabendefinitionen fehl, die Host-Netzwerkmodus- und Container-Definitionen von`privileged=false`, leer und `user=root` oder leer haben.

Dieses Steuerelement bewertet nur die letzte aktive Revision einer Amazon ECS-Aufgabendefinition.

Mit dieser Steuerung soll sichergestellt werden, dass der Zugriff bewusst definiert wird, wenn Sie Aufgaben ausführen, die den Host-Netzwerkmodus verwenden. Wenn eine Aufgabendefinition über erhöhte Rechte verfügt, liegt das daran, dass Sie diese Konfiguration gewählt haben. Dieses Steuerelement sucht nach unerwarteter Rechteerweiterung, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist und Sie keine erhöhten Rechte wählen.

Abhilfe

Informationen zum Aktualisieren einer Aufgabendefinition finden Sie unter Aktualisieren einer Aufgabendefinition im Amazon Elastic Container Service Developer Guide.

Wenn Sie eine Aufgabendefinition aktualisieren, werden laufende Aufgaben, die mit der vorherigen Aufgabendefinition gestartet wurden, nicht aktualisiert. Um eine laufende Aufgabe zu aktualisieren, müssen Sie die Aufgabe mit der neuen Aufgabendefinition erneut bereitstellen.

[ECS.2] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden

Verwandte Anforderungen: NIST.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::ECS::Service`

AWS Config Regel: `ecs-service-assign-public-ip-disabled` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

- `exemptEcsServiceArns`(nicht anpassbar). Security Hub füllt diesen Parameter nicht aus. Durch Kommas getrennte Liste der ARNs von Amazon ECS-Services, die von dieser Regel ausgenommen sind.

  Diese Regel gilt, `COMPLIANT` wenn ein Amazon ECS-Service auf diese Parameterliste `AssignPublicIP` gesetzt wurde `ENABLED` und in dieser angegeben ist.

  Diese Regel gilt, `NON_COMPLIANT` wenn ein Amazon ECS-Service auf `AssignPublicIP` festgelegt wurde `ENABLED` und in dieser Parameterliste nicht angegeben ist.

Dieses Steuerelement prüft, ob die Amazon ECS-Services so konfiguriert sind, dass sie automatisch öffentliche IP-Adressen zuweisen. Diese Steuerung schlägt fehl, wenn dies `AssignPublicIP` der Fall ist`ENABLED`. Diese Kontrolle `AssignPublicIP` ist erfolgreich, falls ja`DISABLED`.

Eine öffentliche IP-Adresse ist eine IP-Adresse, die über das Internet erreichbar ist. Wenn Sie Ihre Amazon ECS-Instances mit einer öffentlichen IP-Adresse starten, sind Ihre Amazon ECS-Instances über das Internet erreichbar. Amazon ECS-Services sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Container-Anwendungsserver ermöglichen kann.

Abhilfe

Informationen zum Deaktivieren der automatischen Zuweisung öffentlicher IP-Adressen finden Sie unter So konfigurieren Sie VPC- und Sicherheitsgruppeneinstellungen für Ihren Service im Amazon Elastic Container Service Developer Guide.

[ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config Regel: ecs-task-definition-pid-mode-check

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Amazon ECS-Aufgabendefinitionen so konfiguriert sind, dass sie den Prozess-Namespace eines Hosts gemeinsam mit seinen Containern verwenden. Die Steuerung schlägt fehl, wenn die Aufgabendefinition den Prozess-Namespace des Hosts gemeinsam mit den darauf laufenden Containern verwendet. Dieses Steuerelement bewertet nur die letzte aktive Revision einer Amazon ECS-Aufgabendefinition.

Ein Prozess-ID-Namespace (PID) sorgt für die Trennung zwischen Prozessen. Er verhindert, dass Systemprozesse sichtbar sind, und ermöglicht die Wiederverwendung von PIDs, einschließlich PID 1. Wenn der PID-Namespace des Hosts gemeinsam mit Containern genutzt wird, könnten Container alle Prozesse auf dem Hostsystem sehen. Dies verringert den Vorteil der Isolierung auf Prozessebene zwischen dem Host und den Containern. Diese Umstände könnten zu unberechtigtem Zugriff auf Prozesse auf dem Host selbst führen, einschließlich der Möglichkeit, diese zu manipulieren und zu beenden. Kunden sollten den Prozess-Namespace des Hosts nicht mit Containern teilen, die darauf laufen.

Abhilfe

Informationen zur Konfiguration der `pidMode` Aufgabendefinition finden Sie unter Aufgabendefinitionsparameter im Amazon Elastic Container Service Developer Guide.

[ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-5, NIST.800-53.r5 AC-6

Kategorie: Schützen > Sichere Zugriffsverwaltung > Zugriffsbeschränkungen für Root-Benutzer

Schweregrad: Hoch

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config-Regel: ecs-containers-nonprivileged

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der `privileged` Parameter in der Container-Definition von Amazon ECS-Aufgabendefinitionen auf gesetzt ist`true`. Die Steuerung schlägt fehl, wenn dieser Parameter gleich ist`true`. Dieses Steuerelement bewertet nur die letzte aktive Revision einer Amazon ECS-Aufgabendefinition.

Wir empfehlen, dass Sie erhöhte Rechte aus Ihren ECS-Aufgabendefinitionen entfernen. Wenn der Berechtigungsparameter laute`true`, erhält der Container erhöhte Rechte auf der Host-Container-Instance (ähnlich wie dem Root-Benutzer).

Abhilfe

Informationen zur Konfiguration des `privileged` Parameters für eine Aufgabendefinition finden Sie unter Erweiterte Container-Definitionsparameter im Amazon Elastic Container Service Developer Guide.

[ECS.5] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-5, NIST.800-53.R5 AC-6

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Hoch

Ressourcentyp: `AWS::ECS::TaskDefinition`

AWS Config-Regel: ecs-containers-readonly-access

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob Amazon ECS-Container auf den schreibgeschützten Zugriff auf bereitgestellte Root-Dateisysteme beschränkt sind. Die Steuerung schlägt fehl, wenn der `readonlyRootFilesystem` Parameter auf gesetzt ist `false` oder wenn der Parameter in der Containerdefinition innerhalb der Aufgabendefinition nicht vorhanden ist. Dieses Steuerelement bewertet nur die letzte aktive Revision einer Amazon ECS-Aufgabendefinition.

Durch die Aktivierung dieser Option werden Sicherheitsangriffsvektoren reduziert, da das Dateisystem der Container-Instance nur manipuliert oder beschrieben werden kann, wenn sie über

explizite Lese- und Schreibberechtigungen für ihren Dateisystemordner und ihre Verzeichnisse verfügt. Diese Steuerung folgt außerdem dem Prinzip der geringsten Rechte.

Abhilfe

Beschränkung von Containerdefinitionen auf den schreibgeschützten Zugriff auf Root-Dateisysteme

1. Öffnen Sie die klassische Amazon-ECS-Konsole unter https://console.aws.amazon.com/ecs/.
2. Wählen Sie im linken Navigationsbereich Aufgabendefinitionen aus.
3. Wählen Sie eine Aufgabendefinition mit Containerdefinitionen aus, die aktualisiert werden müssen. Führen Sie für jeden Schritt die folgenden Schritte aus:
   - Wählen Sie in der Dropdownliste die Option Neue Revision mit JSON erstellen aus.
   - Fügen Sie den `readonlyRootFilesystem` Parameter hinzu und legen Sie ihn `true` in der Containerdefinition innerhalb der Aufgabendefinition auf fest.
   - Wählen Sie Erstellen.

[ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schützen > Sichere Entwicklung > Anmeldeinformationen sind nicht fest codiert

Schweregrad: Hoch

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config-Regel: ecs-no-environment-secrets

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- secretKeys =`AWS_ACCESS_KEY_ID`,`AWS_SECRET_ACCESS_KEY`, `ECS_ENGINE_AUTH_DATA` (nicht anpassbar)

Dieses Steuerelement prüft, ob der Schlüsselwert einer Variablen im `environment` Parameter von ContainerdefinitionenAWS_ACCESS_KEY_ID,AWS_SECRET_ACCESS_KEY,

oder enthält. `ECS_ENGINE_AUTH_DATA` Dieses Steuerelement schlägt fehl, wenn eine einzelne Umgebungsvariable in einer Containerdefinition gleich `AWS_ACCESS_KEY_IDAWS_SECRET_ACCESS_KEY`, oder `ECS_ENGINE_AUTH_DATA` ist. Diese Kontrolle deckt keine Umgebungsvariablen ab, die von anderen Standorten wie Amazon S3 weitergegeben werden. Dieses Steuerelement bewertet nur die letzte aktive Revision einer Amazon ECS-Aufgabendefinition.

AWS Systems Manager Parameter Store kann Ihnen helfen, die Sicherheitslage Ihres Unternehmens zu verbessern. Wir empfehlen, den Parameter Store zum Speichern von Geheimnissen und Anmeldeinformationen zu verwenden, anstatt sie direkt an Ihre Container-Instances zu übergeben oder sie fest in Ihren Code zu codieren.

Abhilfe

Informationen zum Erstellen von Parametern mit SSM finden Sie unter Erstellen von Systems Manager Manager-Parametern im AWS Systems Manager Benutzerhandbuch. Weitere Informationen zum Erstellen einer Aufgabendefinition, die ein Geheimnis spezifiziert, finden Sie unter Spezifying sensitive data using Secrets Manager im Amazon Elastic Container Service Developer Guide.

[ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen

Verwandte Anforderungen: NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-3. R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Hoch

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config Regel: ecs-task-definition-log -Konfiguration

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für die letzte aktive Amazon ECS-Aufgabendefinition eine Protokollierungskonfiguration angegeben wurde. Die Steuerung schlägt fehl, wenn für die

Aufgabendefinition die `logConfiguration` Eigenschaft nicht definiert `logDriver` ist oder wenn der Wert für in mindestens einer Containerdefinition Null ist.

Die Protokollierung hilft Ihnen dabei, die Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon ECS aufrechtzuerhalten. Das Sammeln von Daten aus Aufgabendefinitionen bietet Transparenz, was Ihnen helfen kann, Prozesse zu debuggen und die Ursache von Fehlern zu finden. Wenn Sie eine Protokollierungslösung verwenden, die nicht in der ECS-Aufgabendefinition definiert werden muss (z. B. eine Protokollierungslösung eines Drittanbieters), können Sie diese Steuerung deaktivieren, nachdem Sie sichergestellt haben, dass Ihre Protokolle ordnungsgemäß erfasst und übermittelt wurden.

Abhilfe

Informationen zum Definieren einer Protokollkonfiguration für Ihre Amazon ECS-Aufgabendefinitionen finden Sie unter Angeben einer Protokollkonfiguration in Ihrer Aufgabendefinition im Amazon Elastic Container Service Developer Guide.

[ECS.10] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen

Verwandte Anforderungen: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5)

Kategorie: Identifizieren > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::ECS::Service`

AWS Config-Regel: `ecs-fargate-latest-platform-version`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `latestLinuxVersion: 1.4.0`(nicht anpassbar)
- `latestWindowsVersion: 1.0.0`(nicht anpassbar)

Dieses Steuerelement prüft, ob die Amazon ECS Fargate-Dienste die neueste Version der Fargate-Plattform ausführen. Diese Steuerung schlägt fehl, wenn die Plattformversion nicht die neueste ist.

AWS Fargate Plattformversionen beziehen sich auf eine spezifische Laufzeitumgebung für die Fargate-Task-Infrastruktur, bei der es sich um eine Kombination aus Kernel- und Container-Laufzeitversionen handelt. Neue Plattformversionen werden veröffentlicht, wenn sich die Laufzeitumgebung weiterentwickelt. Beispielsweise kann eine neue Version für Kernel- oder Betriebssystemupdates, neue Funktionen, Bugfixes oder Sicherheitsupdates veröffentlicht werden. Sicherheits-Updates und -Patches für Ihre -Fargate-Aufgaben werden automatisch bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das sich auf eine Plattformversion auswirkt, wird die AWS Plattformversion gepatcht.

Abhilfe

Informationen zum Aktualisieren eines vorhandenen Service, einschließlich seiner Plattformversion, finden Sie unter Aktualisieren eines Service im Amazon Elastic Container Service Developer Guide.

[ECS.12] ECS-Cluster sollten Container Insights verwenden

Verwandte Anforderungen: NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-2

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::ECS::Cluster`

AWS Config-Regel: `ecs-container-insights-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ECS-Cluster Container Insights verwenden. Diese Steuerung schlägt fehl, wenn Container Insights nicht für einen Cluster eingerichtet ist.

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon ECS-Clustern. Verwenden Sie CloudWatch Container Insights, um Metriken und Protokolle aus Ihren containerisierten Anwendungen und Microservices zu sammeln, zu aggregieren und zusammenzufassen. CloudWatch sammelt automatisch Metriken für viele Ressourcen wie CPU, Arbeitsspeicher, Festplatte und Netzwerk. Container Insights bietet auch Diagnoseinformationen, wie z. B.Fehler beim Container-Neustart, damit Sie Probleme schnell aufdecken und beheben können. Sie können auch CloudWatch Alarme für Metriken einrichten, die Container Insights sammelt.

Abhilfe

Informationen zur Verwendung von Container Insights finden Sie unter Service aktualisieren im CloudWatch Amazon-Benutzerhandbuch.

[ECS.13] ECS-Services sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::ECS::Service`

AWS Config Regel: `tagged-ecs-service` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon ECS-Service Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Service keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Dienst mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem ECS-Service finden Sie unter Tagging your Amazon ECS-Ressourcen im Amazon Elastic Container Service Developer Guide.

[ECS.14] ECS-Cluster sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::ECS::Cluster`

AWS Config Regel: `tagged-ecs-cluster` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon ECS-Cluster Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Cluster keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Cluster mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem ECS-Cluster finden Sie unter Tagging your Amazon ECS-Ressourcen im Amazon Elastic Container Service Developer Guide.

[ECS.15] ECS-Aufgabendefinitionen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::ECS::TaskDefinition`

AWS Config Regel: `tagged-ecs-taskdefinition` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon ECS-Aufgabendefinition Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn die Aufgabendefinition keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Aufgabendefinition mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer ECS-Aufgabendefinition finden Sie unter Tagging your Amazon ECS-Ressourcen im Amazon Elastic Container Service Developer Guide.

Amazon Elastic Compute Cloud-Steuerelemente

Diese Kontrollen beziehen sich auf Amazon EC2 EC2-Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[EC2.1] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/7.2.1, NIST.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4, NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 NIst.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `ebs-snapshot-public-restorable-check`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon Elastic Block Store-Snapshots nicht öffentlich sind. Die Kontrolle schlägt fehl, wenn Amazon EBS-Snapshots von jedermann wiederhergestellt werden können.

EBS-Snapshots werden verwendet, um die Daten auf Ihren EBS-Volumes zu einem bestimmten Zeitpunkt auf Amazon S3 zu sichern. Sie können die Snapshots verwenden, um frühere Status von EBS-Volumes wiederherzustellen. Es ist selten akzeptabel, einen Snapshot mit der Öffentlichkeit zu teilen. Typischerweise wurde die Entscheidung, eine Momentaufnahme öffentlich zu teilen, irrtümlich oder ohne vollständiges Verständnis der Auswirkungen getroffen. Diese Überprüfung trägt dazu bei, dass alle diese Freigaben vollständig geplant und beabsichtigt waren.

Informationen dazu, wie Sie einen öffentlichen EBS-Snapshot privat machen können, finden Sie unter Einen Snapshot teilen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances. Wählen Sie für Aktionen, Berechtigungen ändern die Option Privat aus.

[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/2.1, CIS AWS Foundations Benchmark v1.2.0/4.3, CIS Foundations Benchmark v1.4.0/5.3, CIS Foundations Benchmark v3.0.0/5.4, NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 AC-7, NIST.NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (5) AWS AWS

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::SecurityGroup`

AWS Config -Regel: `vpc-default-security-group-closed`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Standardsicherheitsgruppe einer VPC eingehenden oder ausgehenden Datenverkehr zulässt. Die Steuerung schlägt fehl, wenn die Sicherheitsgruppe eingehenden oder ausgehenden Datenverkehr zulässt.

Die Regeln für die Standardsicherheitsgruppe erlauben den gesamten ausgehenden und eingehenden Datenverkehr von Netzwerkschnittstellen (und den zugehörigen Instances), die derselben Sicherheitsgruppe zugewiesen sind. Wir empfehlen, die Standardsicherheitsgruppe nicht zu verwenden. Da die Standardsicherheitsgruppe nicht gelöscht werden kann, sollten Sie die Standardeinstellung für Sicherheitsgruppenregeln ändern, um eingehenden und ausgehenden Datenverkehr einzuschränken. Dies verhindert unbeabsichtigten Datenverkehr, wenn die Standardsicherheitsgruppe versehentlich für Ressourcen wie EC2-Instances konfiguriert ist.

Abhilfe

Um dieses Problem zu beheben, erstellen Sie zunächst neue Sicherheitsgruppen mit den geringsten Rechten. Anweisungen finden Sie unter Erstellen einer Sicherheitsgruppe im Amazon VPC-Benutzerhandbuch. Weisen Sie dann die neuen Sicherheitsgruppen Ihren EC2-Instances zu. Anweisungen finden Sie unter Ändern der Sicherheitsgruppe einer Instance im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

Nachdem Sie Ihren Ressourcen die neuen Sicherheitsgruppen zugewiesen haben, entfernen Sie alle Regeln für eingehenden und ausgehenden Datenverkehr aus den Standardsicherheitsgruppen. Anweisungen finden Sie unter Löschen von Sicherheitsgruppenregeln im Amazon VPC-Benutzerhandbuch.

[EC2.3] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::Volume`

AWS Config -Regel: `encrypted-volumes`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die EBS-Volumes, die sich im angefügten Zustand befinden, verschlüsselt sind. Um diese Prüfung zu bestehen, müssen EBS-Volumes in Betrieb und verschlüsselt sein. Wenn das EBS-Volume nicht angefügt ist, unterliegt es nicht dieser Prüfung.

Um eine zusätzliche Sicherheitsebene Ihrer sensiblen Daten in EBS-Volumes zu gewährleisten, sollten Sie die EBS-Verschlüsselung im Ruhezustand aktivieren. Die Amazon EBS-Verschlüsselung bietet eine einfache Verschlüsselungslösung für Ihre EBS-Ressourcen, ohne dass Sie eine eigene Infrastruktur für die Schlüsselverwaltung erstellen, verwalten und sichern müssen. Bei der Erstellung verschlüsselter Volumes und Snapshots werden KMS-Schlüssel verwendet.

Weitere Informationen zur Amazon EBS-Verschlüsselung finden Sie unter Amazon EBS-Verschlüsselung im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

Abhilfe

Es gibt keine direkte Möglichkeit, ein vorhandenes unverschlüsseltes Volume oder einen Snapshot zu verschlüsseln. Sie können ein neues Volume oder einen neuen Snapshot nur beim Erstellen verschlüsseln.

Wenn Sie die Verschlüsselung standardmäßig aktiviert haben, verschlüsselt Amazon EBS das resultierende neue Volume oder den Snapshot mit Ihrem Standardschlüssel für die Amazon EBS-Verschlüsselung. Auch wenn Sie die standardmäßige Verschlüsselung nicht aktiviert haben, können Sie die Verschlüsselung beim Erstellen eines einzelnen Volumes oder Snapshots aktivieren. In beiden Fällen können Sie den Standardschlüssel für die Amazon EBS-Verschlüsselung überschreiben und einen symmetrischen, vom Kunden verwalteten Schlüssel wählen.

Weitere Informationen finden Sie unter Erstellen eines Amazon EBS-Volumes und Kopieren eines Amazon EBS-Snapshots im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Identifizieren > Bestand

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::Instance`

AWS Config -Regel: `ec2-stopped-instance`

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`AllowedDays`	Anzahl der Tage, an denen sich die EC2-Instance im gestoppten Zustand befinden darf, bevor ein fehlgeschlagenes Ergebnis generiert wird.	Ganzzahl	1 auf 365	30

Diese Kontrolle prüft, ob eine Amazon EC2 EC2-Instance länger als die zulässige Anzahl von Tagen angehalten wurde. Die Kontrolle schlägt fehl, wenn eine EC2-Instance länger als die maximal zulässige Zeitspanne angehalten wird. Sofern Sie keinen benutzerdefinierten Parameterwert für den maximal zulässigen Zeitraum angeben, verwendet Security Hub einen Standardwert von 30 Tagen.

Wenn eine EC2-Instance über einen längeren Zeitraum nicht ausgeführt wurde, stellt dies ein Sicherheitsrisiko dar, da die Instance nicht aktiv gewartet (analysiert, gepatcht, aktualisiert) wird. Wenn sie später gestartet wird, kann der Mangel an ordnungsgemäßer Wartung zu unerwarteten Problemen in Ihrer AWS Umgebung führen. Um eine EC2-Instance über einen längeren Zeitraum sicher inaktiv zu halten, starten Sie sie regelmäßig zu Wartungszwecken und beenden Sie sie dann nach der Wartung. Idealerweise sollte dies ein automatisierter Prozess sein.

Abhilfe

Informationen zum Beenden einer inaktiven EC2-Instance finden Sie unter Terminate an Instance im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/2.9, CIS Foundations Benchmark v1.4.0/3.9, CIS AWS Foundations Benchmark v3.0.0/3.7, PCI DSS v3.2.1/10.3.3, PCI DSS v3.2.1/10.3.4, PCI DSS v3.2.1/10.3.5, PCI DSS v3.2.1/10.3.6, NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-12, NIST.NIST.800-53.r5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-7 (8) AWS

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::VPC`

AWS Config -Regel: `vpc-flow-logs-enabled`

Art des Zeitplans: Periodisch

Parameter:

- `trafficType`: `REJECT` (nicht anpassbar)

Dieses Steuerelement prüft, ob Amazon VPC Flow Logs gefunden und für VPCs aktiviert wurden. Der Verkehrstyp ist auf eingestellt. `Reject`

Mit der Funktion VPC Flow Logs können Sie Informationen über den IP-Adressverkehr zu und von Netzwerkschnittstellen in Ihrer VPC erfassen. Nachdem Sie ein Flow-Protokoll erstellt haben, können Sie die zugehörigen Daten in CloudWatch Logs anzeigen und abrufen. Um die Kosten zu senken, können Sie Ihre Flow-Logs auch an Amazon S3 senden.

Security Hub empfiehlt, die Flussprotokollierung für Paketablehnungen für VPCs zu aktivieren. Flow-Logs bieten Einblick in den Netzwerkverkehr, der die VPC durchquert, und können anomalen Datenverkehr erkennen oder Einblicke in Sicherheitsworkflows geben.

Standardmäßig enthält der Datensatz Werte für die verschiedenen Komponenten des IP-Adressflusses, einschließlich Quelle, Ziel und Protokoll. Weitere Informationen und Beschreibungen der Protokollfelder finden Sie unter VPC Flow Logs im Amazon VPC-Benutzerhandbuch.

Abhilfe

Informationen zum Erstellen eines VPC-Flow-Protokolls finden Sie unter Erstellen eines Flow-Protokolls im Amazon VPC-Benutzerhandbuch. Nachdem Sie die Amazon VPC-Konsole geöffnet haben, wählen Sie Your VPCs. Wählen Sie für Filter die Option Ablehnen oder Alle.

[EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.4.0/2.2.1, CIS AWS Foundations Benchmark v3.0.0/2.2.1, NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIst.800-53.R5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `ec2-ebs-encryption-by-default`

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob die Verschlüsselung auf Kontoebene standardmäßig für Amazon Elastic Block Store (Amazon EBS) aktiviert ist. Die Kontrolle schlägt fehl, wenn die Verschlüsselung auf Kontoebene nicht aktiviert ist.

Wenn die Verschlüsselung für Ihr Konto aktiviert ist, werden Amazon EBS-Volumes und Snapshot-Kopien im Ruhezustand verschlüsselt. Dies bietet eine zusätzliche Schutzebene für Ihre Daten. Weitere Informationen dazu finden Sie unter Gerätebenennung bei Linux-Instances im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

Beachten Sie, dass die folgenden Instance-Typen keine Verschlüsselung unterstützen: R1, C1 und M1.

Abhilfe

Informationen zur Konfiguration der Standardverschlüsselung für Amazon EBS-Volumes finden Sie unter Standardverschlüsselung im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/5.6, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::Instance`

AWS Config -Regel: `ec2-imdsv2-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Ihre EC2-Instance-Metadatenversion mit Instance Metadata Service Version 2 (IMDSv2) konfiguriert ist. Das Steuerelement ist erfolgreich, wenn `HttpTokens` es für IMDSv2 auf erforderlich gesetzt ist. Das Steuerelement schlägt fehl, wenn auf gesetzt `HttpTokens` ist. `optional`

Sie verwenden Instanz-Metadaten, um die laufende Instanz zu konfigurieren oder zu verwalten. Das IMDS bietet Zugriff auf temporäre, häufig wechselnde Anmeldeinformationen. Mit diesen

Anmeldeinformationen entfällt die Notwendigkeit, vertrauliche Anmeldeinformationen manuell oder programmgesteuert fest zu codieren oder vertrauliche Anmeldeinformationen an Instanzen zu verteilen. Das IMDS ist lokal an jede EC2-Instance angehängt. Es läuft auf einer speziellen „Link Local“ -IP-Adresse 169.254.169.254. Auf diese IP-Adresse kann nur mit Software zugegriffen werden, die auf der Instance ausgeführt wird.

Version 2 des IMDS bietet neue Schutzmaßnahmen für die folgenden Arten von Sicherheitslücken. Diese Sicherheitslücken könnten genutzt werden, um zu versuchen, auf das IMDS zuzugreifen.

- Öffnen Sie die Firewalls für Websites und Anwendungen.
- Öffnen Sie Reverse-Proxys
- Sicherheitslücken bei serverseitiger Anforderungsfälschung (SSRF)
- Offene Layer-3-Firewalls und Network Address Translation (NAT)

Security Hub empfiehlt, dass Sie Ihre EC2-Instances mit IMDSv2 konfigurieren.

Abhilfe

Informationen zur Konfiguration von EC2-Instances mit IMDSv2 finden Sie unter Empfohlener Pfad zur Anforderung von IMDSv2 im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.9] Amazon EC2 EC2-Instances sollten keine öffentliche IPv4-Adresse haben

Verwandte Anforderungen: NIST.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Öffentliche IP-Adressen

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::Instance`

AWS Config -Regel: `ec2-instance-no-public-ip`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob EC2-Instances eine öffentliche IP-Adresse haben. Die Steuerung schlägt fehl, wenn das `publicIp` Feld im EC2-Instance-Konfigurationselement vorhanden ist. Dieses Steuerelement gilt nur für IPv4-Adressen.

Eine öffentliche IPv4-Adresse ist eine IP-Adresse, die über das Internet erreichbar ist. Wenn Sie Ihre Instance mit einer öffentlichen IP-Adresse starten, ist Ihre EC2-Instance über das Internet erreichbar. Eine private IPv4-Adresse ist eine IP-Adresse, die über das Internet nicht erreichbar ist. Sie können private IPv4-Adressen für die Kommunikation zwischen EC2-Instances in derselben VPC oder in Ihrem verbundenen privaten Netzwerk verwenden.

IPv6-Adressen sind weltweit einzigartig und daher über das Internet erreichbar. Standardmäßig ist das IPv6-Adressierungsattribut jedoch in allen Subnetzen auf False gesetzt. Weitere Informationen zu IPv6 finden Sie unter IP-Adressierung in Ihrer VPC im Amazon VPC-Benutzerhandbuch.

Wenn Sie einen legitimen Anwendungsfall für die Verwaltung von EC2-Instances mit öffentlichen IP-Adressen haben, können Sie die Ergebnisse dieser Kontrolle unterdrücken. Weitere Informationen zu Front-End-Architekturoptionen finden Sie im AWS Architektur-Blog oder in der Reihe This Is My Architecture.

Abhilfe

Verwenden Sie eine nicht standardmäßige VPC, sodass Ihrer Instance standardmäßig keine öffentliche IP-Adresse zugewiesen wird.

Wenn Sie eine EC2-Instance in einer Standard-VPC VPC, wird ihr eine öffentliche IP-Adresse zugewiesen. Wenn Sie eine EC2-Instance in einer nicht standardmäßigen VPC starten, bestimmt die Subnetzkonfiguration, ob sie eine öffentliche IP-Adresse erhält. Das Subnetz verfügt über ein Attribut, das bestimmt, ob neue EC2-Instances im Subnetz eine öffentliche IP-Adresse aus dem öffentlichen IPv4-Adresspool erhalten.

Sie können eine automatisch zugewiesene öffentliche IP-Adresse Ihrer EC2-Instance nicht manuell zuordnen oder trennen. Gehen Sie wie folgt vor, um zu kontrollieren, ob Ihre EC2-Instance eine öffentliche IP-Adresse erhält:

- Ändern Sie das öffentliche IP-Adressierungsattribut Ihres Subnetzes. Weitere Informationen finden Sie unter Ändern des öffentlichen IPv4-Adressierungsattributs für Ihr Subnetz in Amazon VPC Benutzerhandbuch.
- Aktivieren oder deaktivieren Sie die Funktion zur öffentlichen IP-Adressierung beim Start. Dadurch wird das öffentliche IP-Adressierungsattribut des Subnetzes außer Kraft gesetzt. Weitere

Informationen finden Sie unter Zuweisen einer öffentlichen IPv4-Adresse beim Instance-Start im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

Weitere Informationen finden Sie unter Öffentliche IPv4-Adressen und externe DNS-Hostnamen im Amazon EC2-Benutzerhandbuch für Linux-Instances.

Wenn Ihre EC2-Instance mit einer Elastic IP-Adresse verknüpft ist, ist Ihre EC2-Instance über das Internet erreichbar. Sie können die Zuordnung einer Elastic IP-Adresse jederzeit von einer Instance oder einer Netzwerkschnittstelle trennen. Informationen zum Trennen einer Elastic IP-Adresse finden Sie unter Trennen einer Elastic IP-Adresse im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.10] Amazon EC2 sollte so konfiguriert sein, dass es VPC-Endpunkte verwendet, die für den Amazon EC2-Service erstellt wurden

Verwandte Anforderungen: NIST.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4)

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Privater API-Zugriff

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::VPC`

AWS Config -Regel: `service-vpc-endpoint-enabled`

Art des Zeitplans: Periodisch

Parameter:

- `serviceName`: `ec2` (nicht anpassbar)

Dieses Steuerelement prüft, ob für jede VPC ein Service-Endpunkt für Amazon EC2 erstellt wurde. Die Steuerung schlägt fehl, wenn für eine VPC kein VPC-Endpunkt für den Amazon EC2-Service erstellt wurde.

Diese Kontrolle bewertet Ressourcen in einem einzigen Konto. Es kann keine Ressourcen beschreiben, die sich außerhalb des Kontos befinden. Da AWS Config Security Hub keine

kontoübergreifenden Prüfungen durchführt, werden Ihnen `FAILED` Ergebnisse für VPCs angezeigt, die von mehreren Konten gemeinsam genutzt werden. Security Hub empfiehlt, diese `FAILED` Ergebnisse zu unterdrücken.

Um die Sicherheitslage Ihrer VPC zu verbessern, können Sie Amazon EC2 so konfigurieren, dass es einen VPC-Schnittstellen-Endpunkt verwendet. Schnittstellenendpunkte werden von einer Technologie unterstützt AWS PrivateLink, mit der Sie privat auf Amazon EC2 EC2-API-Operationen zugreifen können. Es schränkt den gesamten Netzwerkverkehr zwischen Ihrer VPC und Amazon EC2 auf das Amazon-Netzwerk ein. Da Endpoints nur in derselben Region unterstützt werden, können Sie keinen Endpunkt zwischen einer VPC und einem Service in einer anderen Region erstellen. Dies verhindert unbeabsichtigte Amazon EC2 EC2-API-Aufrufe in andere Regionen.

Weitere Informationen zum Erstellen von VPC-Endpunkten für Amazon EC2 finden Sie unter Amazon EC2 und Interface-VPC-Endpoints im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

Abhilfe

Informationen zum Erstellen eines Schnittstellenendpunkts zu Amazon EC2 über die Amazon VPC-Konsole finden Sie unter Erstellen eines VPC-Endpunkts im Handbuch.AWS PrivateLink Wählen Sie für den Servicenamen com.amazonaws aus. ***region .ec2.***

Sie können auch eine Endpunktrichtlinie erstellen und an Ihren VPC-Endpunkt anhängen, um den Zugriff auf die Amazon EC2 EC2-API zu kontrollieren. Anweisungen zum Erstellen einer VPC-Endpunktrichtlinie finden Sie unter Erstellen einer Endpunktrichtlinie im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.12] Ungenutzte Amazon EC2 EC2-EIPs sollten entfernt werden

Verwandte Anforderungen: PCI DSS v3.2.1/2.4, NIST.800-53.R5 CM-8 (1)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::EIP`

AWS Config -Regel: `eip-attached`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Elastic IP (EIP) -Adressen, die einer VPC zugewiesen sind, an EC2-Instances oder verwendete Elastic Network Interfaces (ENIs) angehängt sind.

Ein fehlgeschlagener Befund deutet darauf hin, dass Sie möglicherweise ungenutzte EC2-EIPs haben.

Auf diese Weise können Sie ein genaues Inventar der EIPs in Ihrer Karteninhaberdatenumgebung (CDE) verwalten.

Informationen zur Freigabe einer ungenutzten EIP finden Sie unter Elastic IP Address veröffentlichen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/4.1, PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/2.2.2, NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 CM-7, NIST.800-53.r5 SC-7, NIST.800-53.r5 R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (5)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::SecurityGroup`

AWS Config -Regel: `restricted-ssh`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon EC2-Sicherheitsgruppe den Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulässt. Die Kontrolle schlägt fehl, wenn die Sicherheitsgruppe den Zugriff von 0.0.0.0/0 oder: :/0 zu Port 22 zulässt.

Sicherheitsgruppen bieten eine zustandsorientierte Filterung von ein- und ausgehendem Netzwerkdatenverkehr von bzw. an AWS -Ressourcen. Unsere Empfehlung ist, dass keine Sicherheitsgruppe uneingeschränkten Zugriff auf Port 22 für eingehenden Datenverkehr erlauben sollte. Durch die Unterbindung der uneingeschränkten Konnektivität mit Remote-Konsolenservices wie SSH wird die Risikoaussetzung eines Servers reduziert.

Abhilfe

Um den Zugriff auf Port 22 zu verhindern, entfernen Sie die Regel, die diesen Zugriff für jede Sicherheitsgruppe, die einer VPC zugeordnet ist, erlaubt. Anweisungen finden Sie unter Sicherheitsgruppenregeln aktualisieren im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances. Nachdem Sie in der Amazon EC2 EC2-Konsole eine Sicherheitsgruppe ausgewählt haben, wählen Sie Aktionen, Regeln für eingehenden Datenverkehr bearbeiten. Entfernen Sie die Regel, die den Zugriff auf Port 22 ermöglicht.

[EC2.14] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulassen

Verwandte Anforderungen: AWS CIS Foundations Benchmark v1.2.0/4.2

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::SecurityGroup`

AWS Config Regel: **`restricted-common-ports`**(Die erstellte Regel ist`restricted-rdp`)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon EC2-Sicherheitsgruppe den Zugriff von 0.0.0.0/0 oder: :/0 zu Port 3389 zulässt. Die Kontrolle schlägt fehl, wenn die Sicherheitsgruppe den Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulässt.

Sicherheitsgruppen bieten eine zustandsorientierte Filterung von ein- und ausgehendem Netzwerkdatenverkehr von bzw. an AWS -Ressourcen. Unsere Empfehlung ist, dass keine Sicherheitsgruppe uneingeschränkten Zugriff auf Port 3389 für eingehenden Datenverkehr erlauben sollte. Durch die Unterbindung der uneingeschränkten Konnektivität mit Remote-Konsolenservices wie RDP wird die Risikoaussetzung eines Servers reduziert.

Abhilfe

Um den Zugriff auf Port 3389 zu verhindern, entfernen Sie die Regel, die diesen Zugriff für jede Sicherheitsgruppe, die einer VPC zugeordnet ist, erlaubt. Anweisungen finden Sie unter Sicherheitsgruppenregeln aktualisieren im Amazon VPC-Benutzerhandbuch. Nachdem Sie in der

Amazon VPC-Konsole eine Sicherheitsgruppe ausgewählt haben, wählen Sie Aktionen, Regeln für eingehenden Datenverkehr bearbeiten. Entfernen Sie die Regel, die den Zugriff auf Port 3389 ermöglicht.

[EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen

Verwandte Anforderungen: NIST.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::Subnet`

AWS Config -Regel: `subnet-auto-assign-public-ip-disabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Zuweisung von öffentlichen IPs in Amazon Virtual Private Cloud (Amazon VPC) -Subnetzen auf `MapPublicIpOnLaunch` eingestellt ist. `FALSE` Die Kontrolle ist erfolgreich, wenn das Flag auf gesetzt ist. `FALSE`

Alle Subnetze haben ein Attribut, das bestimmt, ob eine im Subnetz erstellte Netzwerkschnittstelle automatisch eine öffentliche IPv4-Adresse erhält. Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Abhilfe

Informationen zur Konfiguration eines Subnetzes, sodass keine öffentlichen IP-Adressen zugewiesen werden, finden Sie unter Ändern des öffentlichen IPv4-Adressierungsattributs für Ihr Subnetz im Amazon VPC-Benutzerhandbuch. Deaktivieren Sie das Kontrollkästchen Automatische Zuweisung einer öffentlichen IPv4-Adresse aktivieren.

[EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden

Verwandte Anforderungen: NIST.800-53.R5 CM-8 (1)

Kategorie: Vorbeugen > Netzwerksicherheit

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::NetworkAcl`

AWS Config -Regel: `vpc-network-acl-unused-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ungenutzte Network Access Control Lists (ACLs) vorhanden sind.

Das Steuerelement überprüft die Elementkonfiguration der Ressource `AWS::EC2::NetworkAcl` und bestimmt die Beziehungen der Netzwerk-ACL.

Wenn die einzige Beziehung die VPC der Netzwerk-ACL ist, schlägt die Steuerung fehl.

Wenn andere Beziehungen aufgeführt sind, ist die Kontrolle erfolgreich.

Abhilfe

Anweisungen zum Löschen einer ungenutzten Netzwerk-ACL finden Sie unter Löschen einer Netzwerk-ACL im Amazon VPC-Benutzerhandbuch. Sie können die Standard-Netzwerk-ACL oder eine ACL, die Subnetzen zugeordnet ist, nicht löschen.

[EC2.17] Amazon EC2 EC2-Instances sollten nicht mehrere ENIs verwenden

Verwandte Anforderungen: NIST.800-53.R5 AC-4 (21)

Kategorie: Netzwerksicherheit

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::Instance`

AWS Config -Regel: `ec2-instance-multiple-eni-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `Adapterids` — Eine Liste von Netzwerkschnittstellen-IDs, die an EC2-Instances angehängt sind (nicht anpassbar)

Dieses Steuerelement prüft, ob eine EC2-Instance mehrere Elastic Network Interfaces (ENIs) oder Elastic Fabric Adapters (EFAs) verwendet. Dieses Steuerelement ist erfolgreich, wenn ein einziger Netzwerkadapter verwendet wird. Das Steuerelement enthält eine optionale Parameterliste zur Identifizierung der zulässigen ENIs. Diese Kontrolle schlägt auch fehl, wenn eine EC2-Instance, die zu einem Amazon EKS-Cluster gehört, mehr als eine ENI verwendet. Wenn Ihre EC2-Instances mehrere ENIs als Teil eines Amazon EKS-Clusters benötigen, können Sie diese Kontrollergebnisse unterdrücken.

Mehrere ENIs können zu doppelt vernetzten Instances führen, d. h. zu Instances mit mehreren Subnetzen. Dies kann die Komplexität der Netzwerksicherheit erhöhen und unbeabsichtigte Netzwerkpfade und Zugriffe zur Folge haben.

Abhilfe

Informationen zum Trennen einer Netzwerkschnittstelle von einer EC2-Instance finden Sie unter Trennen einer Netzwerkschnittstelle von einer Instance im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen

Verwandte Anforderungen: NIst.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (5)

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Sicherheitsgruppenkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::SecurityGroup`

AWS Config -Regel: `vpc-sg-open-only-to-authorized-ports`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`authorizedTcpPorts`	Liste der autorisierten TCP-Ports	IntegerList (maximal 32 Artikel)	1 auf `65535`	`[80,443]`
`authorizedUdpPorts`	Liste der autorisierten UDP-Ports	IntegerList (maximal 32 Artikel)	1 auf `65535`	Kein Standardwert

Diese Kontrolle prüft, ob eine Amazon EC2-Sicherheitsgruppe uneingeschränkten eingehenden Datenverkehr von nicht autorisierten Ports zulässt. Der Kontrollstatus wird wie folgt bestimmt:

- Wenn Sie den Standardwert für verwenden`authorizedTcpPorts`, schlägt die Steuerung fehl, wenn die Sicherheitsgruppe uneingeschränkten eingehenden Verkehr von einem anderen Port als den Ports 80 und 443 zulässt.
- Wenn Sie benutzerdefinierte Werte für `authorizedTcpPorts` oder angeben, schlägt die Steuerung fehl`authorizedUdpPorts`, wenn die Sicherheitsgruppe uneingeschränkten eingehenden Verkehr von einem nicht aufgelisteten Port zulässt.
- Wenn kein Parameter verwendet wird, schlägt die Steuerung für jede Sicherheitsgruppe fehl, für die eine Regel für uneingeschränkten eingehenden Verkehr gilt.

Sicherheitsgruppen bieten eine statusabhängige Filterung von eingehendem und ausgehendem Netzwerkverkehr zu. AWS Sicherheitsgruppenregeln sollten dem Prinzip des Zugriffs mit den geringsten Rechten folgen. Uneingeschränkter Zugriff (IP-Adresse mit dem Suffix /0) erhöht die Wahrscheinlichkeit bösartiger Aktivitäten wie Hacking, denial-of-service Angriffe und Datenverlust. Sofern ein Port nicht ausdrücklich zugelassen ist, sollte der Port den uneingeschränkten Zugriff verweigern.

Abhilfe

Informationen zum Ändern einer Sicherheitsgruppe finden Sie unter Arbeiten mit Sicherheitsgruppen im Amazon VPC-Benutzerhandbuch.

[EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen

Verwandte Anforderungen: NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 CA-9 (1), NIst.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2), NIst.800-53.R5 CM-7, NIst.800-53.R5 SC-7, NIst.800-53.R5 SC-7, NIst.NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (5)

Kategorie: Schützen > Eingeschränkter Netzwerkzugriff

Schweregrad: Kritisch

Art der Ressource: `AWS::EC2::SecurityGroup`

AWS Config Regel: **`restricted-common-ports`**(Die erstellte Regel ist`vpc-sg-restricted-common-ports`)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: `"blockedPorts": "20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,560` (nicht anpassbar)

Diese Kontrolle prüft, ob uneingeschränkter eingehender Verkehr für eine Amazon EC2-Sicherheitsgruppe für die angegebenen Ports, die als risikoreich gelten, zugänglich ist. Diese Kontrolle schlägt fehl, wenn eine der Regeln in einer Sicherheitsgruppe eingehenden Datenverkehr von '0.0.0.0/0' oder ': :/0' zu diesen Ports zulässt.

Sicherheitsgruppen bieten eine zustandsorientierte Filterung von ein- und ausgehendem Netzwerkdatenverkehr von bzw. an AWS -Ressourcen. Uneingeschränkter Zugriff (0.0.0.0/0) erhöht die Wahrscheinlichkeit bösartiger Aktivitäten wie Hacking, Angriffe und Datenverlust. denial-of-service Keine Sicherheitsgruppe sollte uneingeschränkten Zugriff auf die folgenden Ports zulassen:

- 20, 21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)
- 110 (POP 3)
- 135 (PRO STÜCK)

- 143 (IMAP)
- 445 (CIFS)
- 1433, 1434 (MSSQL)
- 3000 (Go-, Node.js- und Ruby-Frameworks für die Webentwicklung)
- 3306 (MySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000 (Python-Frameworks für die Webentwicklung)
- 5432 (Postgresql)
- 5500 (1) fcp-addr-srvr
- 5601 (Armaturenbretter) OpenSearch
- 8080 (Proxy)
- 8088 (älterer HTTP-Port)
- 8888 (alternativer HTTP-Port)
- 9200 oder 9300 () OpenSearch

Abhilfe

Informationen zum Löschen von Regeln aus einer Sicherheitsgruppe finden Sie unter Regeln aus einer Sicherheitsgruppe löschen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.20] Beide VPN-Tunnel für eine AWS Site-to-Site-VPN-Verbindung sollten aktiv sein

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Ausfallsicherheit > Wiederherstellung > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::VPNConnection`

AWS Config -Regel: `vpc-vpn-2-tunnels-up`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Ein VPN-Tunnel ist eine verschlüsselte Verbindung, über die Daten vom Kundennetzwerk zu oder AWS innerhalb einer AWS Site-to-Site-VPN-Verbindung übertragen werden können. Jede VPN-Verbindung umfasst zwei VPN-Tunnel, die Sie für eine hohe Verfügbarkeit gleichzeitig verwenden können. Es ist wichtig, sicherzustellen, dass beide VPN-Tunnel für eine VPN-Verbindung verfügbar sind, um eine sichere und hochverfügbare Verbindung zwischen einer AWS VPC und Ihrem Remote-Netzwerk zu bestätigen.

Dieses Steuerelement überprüft, ob sich beide von AWS Site-to-Site VPN bereitgestellten VPN-Tunnel im Status UP befinden. Die Steuerung schlägt fehl, wenn sich einer oder beide Tunnel im Status DOWN befinden.

Abhilfe

Informationen zum Ändern der VPN-Tunneloptionen finden Sie unter Ändern der Site-to-Site-VPN-Tunneloptionen im AWS Site-to-Site-VPN-Benutzerhandbuch.

[EC2.21] Netzwerk-ACLs sollten keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.4.0/5.1, CIS AWS Foundations Benchmark v3.0.0/5.1, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2), NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7, NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (5)

Kategorie: Schützen > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::NetworkAcl`

AWS Config -Regel: `nacl-no-unrestricted-ssh-rdp`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Network Access Control List (NACL) uneingeschränkten Zugriff auf die Standard-TCP-Ports für eingehenden SSH/RDP-Verkehr ermöglicht. Die Regel schlägt fehl, wenn ein eingehender NACL-Eintrag einen Quell-CIDR-Block von '0.0.0.0/0' oder ': :/0' für die TCP-Ports 22 oder 3389 zulässt.

Der Zugriff auf Remoteserveradministrationsports, wie Port 22 (SSH) und Port 3389 (RDP), sollte nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ressourcen innerhalb Ihrer VPC ermöglichen kann.

Abhilfe

Weitere Informationen zu NACLs finden Sie unter Netzwerk-ACLs im VPC-Benutzerhandbuch.

[EC2.22] Ungenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden

> **Important**
>
> AUS BESTIMMTEN STANDARDS AUSGESCHLOSSEN — Security Hub hat diese Kontrolle am 20. September 2023 aus dem Standard AWS Foundational Security Best Practices und der NIST SP 800-53 Rev. 5 entfernt. Dieses Steuerelement ist immer noch Teil des Service-Managed Standard:. AWS Control Tower Dieses Steuerelement führt zu einer bestandenen Feststellung, ob Sicherheitsgruppen an EC2-Instances oder an eine elastic network interface angehängt sind. In bestimmten Anwendungsfällen stellen nicht verknüpfte Sicherheitsgruppen jedoch kein Sicherheitsrisiko dar. Sie können andere EC2-Steuerelemente wie EC2.2, EC2.13, EC2.14, EC2.18 und EC2.19 verwenden, um Ihre Sicherheitsgruppen zu überwachen.

Kategorie: Identifizieren > Bestand

Schweregrad: Mittel

`AWS::EC2::NetworkInterface`Ressourcentyp:, `AWS::EC2::SecurityGroup`

AWS Config -Regel: `ec2-security-group-attached-to-eni-periodic`

Art des Zeitplans: Periodisch

Parameter: Keine

Diese AWS Kontrolle überprüft, ob Sicherheitsgruppen an Amazon Elastic Compute Cloud (Amazon EC2) -Instances oder an eine elastic network interface angehängt sind. Die Kontrolle schlägt fehl, wenn die Sicherheitsgruppe keiner Amazon EC2 EC2-Instance oder einer elastic network interface zugeordnet ist.

Abhilfe

Informationen zum Erstellen, Zuweisen und Löschen von Sicherheitsgruppen finden Sie unter Sicherheitsgruppen im Amazon EC2 EC2-Benutzerhandbuch.

[EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren

Verwandte Anforderungen: NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::TransitGateway`

AWS Config -Regel: `ec2-transit-gateway-auto-vpc-attach-disabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob EC2-Transit-Gateways gemeinsam genutzte VPC-Anhänge automatisch akzeptieren. Diese Steuerung schlägt bei einem Transit-Gateway fehl, das automatisch gemeinsame VPC-Anhangsanforderungen akzeptiert.

Durch die Aktivierung wird ein Transit-Gateway so `AutoAcceptSharedAttachments` konfiguriert, dass es automatisch alle kontoübergreifenden VPC-Anhangsanforderungen akzeptiert, ohne die Anfrage oder das Konto, von dem der Anhang stammt, zu überprüfen. Um den bewährten Methoden der Autorisierung und Authentifizierung zu folgen, empfehlen wir, diese Funktion zu deaktivieren, um sicherzustellen, dass nur autorisierte VPC-Anhangsanfragen akzeptiert werden.

Abhilfe

Informationen zum Ändern eines Transit-Gateways finden Sie unter Modifizieren eines Transit-Gateways im Amazon VPC Developer Guide.

[EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden

Verwandte Anforderungen: NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Identifizieren > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::EC2::Instance`

AWS Config -Regel: `ec2-paravirtual-instance-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Virtualisierungstyp einer EC2-Instance paravirtuell ist. Die Steuerung schlägt fehl, wenn der Wert `virtualizationType` der EC2-Instance auf gesetzt ist. `paravirtual`

Linux Amazon Machine Images (AMIs) verwenden eine von zwei Arten der Virtualisierung: paravirtuelle (PV) oder virtuelle Hardware-Maschine (HVM). Die Hauptunterschiede zwischen PV- und HVM-AMIs sind die Art und Weise, wie sie gestartet werden und ob sie spezielle Hardwareerweiterungen (CPU, Netzwerk und Speicher) zur Verbesserung der Leistung nutzen können.

Früher verfügten PV-Gäste in vielen Fällen über eine bessere Leistung als HVM-Gäste, aber aufgrund von Verbesserungen der HVM-Virtualisierung und der Verfügbarkeit von PV-Treibern für HVM-AMIs ist dies nicht mehr der Fall. Weitere Informationen finden Sie unter Linux-AMI-Virtualisierungstypen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

Abhilfe

Informationen zum Aktualisieren einer EC2-Instance auf einen neuen Instance-Typ finden Sie unter Ändern des Instance-Typs im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen

Verwandte Anforderungen: NIST.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::LaunchTemplate`

AWS Config -Regel: `ec2-launch-template-public-ip-disabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon EC2 EC2-Startvorlagen so konfiguriert sind, dass Netzwerkschnittstellen beim Start öffentliche IP-Adressen zugewiesen werden. Die Steuerung schlägt fehl, wenn eine EC2-Startvorlage so konfiguriert ist, dass sie Netzwerkschnittstellen eine öffentliche IP-Adresse zuweist, oder wenn mindestens eine Netzwerkschnittstelle mit einer öffentlichen IP-Adresse vorhanden ist.

Eine öffentliche IP-Adresse ist eine, die über das Internet erreichbar ist. Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die mit diesen Netzwerkschnittstellen verknüpften Ressourcen möglicherweise vom Internet aus erreichbar. EC2-Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Workloads ermöglichen kann.

Abhilfe

Informationen zum Aktualisieren einer EC2-Startvorlage finden Sie unter Ändern der Standardeinstellungen für die Netzwerkschnittstelle im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

[EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6, NIST.800-53.R5 CP-6 (1), NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 CP-9, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::Volume`

AWS Config Regel: `ebs-resources-protected-by-backup-plan`

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`backupVaultLockCheck`	Das Steuerelement ermittelt, `PASSED` ob der Parameter auf gesetzt ist `true` und die Ressource AWS Backup Vault Lock verwendet.	Boolesch	`true` oder `false`	Kein Standardwert

Diese Kontrolle bewertet, ob ein Amazon EBS-Volume, das sich im `in-use` Status befindet, durch einen Backup-Plan abgedeckt ist. Die Kontrolle schlägt fehl, wenn ein EBS-Volume nicht durch einen Backup-Plan abgedeckt ist. Wenn Sie den `backupVaultLockCheck` Parameter auf gleich setzen`true`, ist die Steuerung nur erfolgreich, wenn das EBS-Volume in einem AWS Backup gesperrten Tresor gesichert ist.

Mithilfe von Backups können Sie sich nach einem Sicherheitsvorfall schneller erholen. Sie stärken auch die Widerstandsfähigkeit Ihrer Systeme. Wenn Sie Amazon EBS-Volumes in einen Backup-Plan aufnehmen, können Sie Ihre Daten vor unbeabsichtigtem Verlust oder Löschung schützen.

Abhilfe

Informationen zum Hinzufügen eines Amazon EBS-Volumes zu einem AWS Backup Backup-Plan finden Sie unter Zuweisen von Ressourcen zu einem Backup-Plan im AWS Backup Entwicklerhandbuch.

[EC2.33] EC2 Transit Gateway-Anhänge sollten markiert werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::TransitGatewayAttachment`

AWS Config Regel: `tagged-ec2-transitgatewayattachment` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EC2-Transit-Gateway-Anhang Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Kontrolle schlägt fehl, wenn der Transit-Gateway-Anhang keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft die Steuerung nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Transit-Gateway-Anhang mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen

möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2-Transit-Gateway-Anhang finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.34] Die Routentabellen des EC2-Transit-Gateways sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::TransitGatewayRouteTable`

AWS Config Regel: `tagged-ec2-transitgatewayroutetable` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource	StringList	Liste der Tags, die	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.		die AWS Anforderungen erfüllen	

Dieses Steuerelement prüft, ob eine Amazon EC2-Transit-Gateway-Routentabelle Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Transit-Gateway-Routentabelle keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Transit-Gateway-Routentabelle mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter

AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2-Transit-Gateway-Routentabelle finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.35] EC2-Netzwerkschnittstellen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::NetworkInterface`

AWS Config Regel: `tagged-ec2-networkinterface` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2 EC2-Netzwerkschnittstelle Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Netzwerkschnittstelle keine Tag-Schlüssel hat oder wenn sie nicht

alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Netzwerkschnittstelle mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2-Netzwerkschnittstelle finden Sie unter Taggen Ihrer Amazon EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.36] EC2-Kunden-Gateways sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::CustomerGateway`

AWS Config Regel: `tagged-ec2-customergateway` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EC2 EC2-Kunden-Gateway Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Kontrolle schlägt fehl, wenn das Kunden-Gateway keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Kunden-Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2-Kunden-Gateway finden Sie unter Taggen Ihrer Amazon EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.37] EC2-Elastic-IP-Adressen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::EIP`

AWS Config Regel: `tagged-ec2-eip` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2 Elastic IP-Adresse Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Elastic IP-Adresse keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Elastic IP-Adresse mit keinem Schlüssel gekennzeichnet ist. System-Tags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2-Elastic-IP-Adresse finden Sie unter Taggen Ihrer Amazon EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.38] EC2-Instances sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::Instance`

AWS Config Regel: `tagged-ec2-instance` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2 EC2-Instance Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Instance keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Instanz mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2-Instance finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.39] EC2-Internet-Gateways sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::InternetGateway`

AWS Config Regel: `tagged-ec2-internetgateway` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList	Liste der Tags, die die AWS	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen	

Dieses Steuerelement prüft, ob ein Amazon EC2 EC2-Internet-Gateway Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn das Internet-Gateway keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Internet-Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2-Internet-Gateway finden Sie unter Taggen Ihrer Amazon EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.40] EC2-NAT-Gateways sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::NatGateway`

AWS Config Regel: `tagged-ec2-natgateway` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EC2 EC2-Gateway zur Netzwerkadressübersetzung (NAT) Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn das NAT-Gateway keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das NAT-Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2-NAT-Gateway finden Sie unter Taggen Ihrer Amazon EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.41] EC2-Netzwerk-ACLs sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::NetworkAcl`

AWS Config Regel: `tagged-ec2-networkacl` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2 EC2-Netzwerkzugriffskontrollliste (Network ACL) Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Kontrolle schlägt fehl, wenn die Netzwerk-ACL keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Netzwerk-ACL mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2-Netzwerk-ACL finden Sie unter Taggen Ihrer Amazon EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.42] EC2-Routing-Tabellen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::RouteTable`

AWS Config Regel: `tagged-ec2-routetable` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2 EC2-Routentabelle Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Routing-Tabelle keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Routing-Tabelle mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2-Routing-Tabelle finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.43] EC2-Sicherheitsgruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::SecurityGroup`

AWS Config Regel: `tagged-ec2-securitygroup` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2-Sicherheitsgruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Kontrolle schlägt fehl, wenn die Sicherheitsgruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Sicherheitsgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer EC2-Sicherheitsgruppe finden Sie unter Taggen Ihrer Amazon EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.44] EC2-Subnetze sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::Subnet`

AWS Config Regel: `tagged-ec2-subnet` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList	Liste der Tags, die die AWS	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen	

Dieses Steuerelement prüft, ob ein Amazon EC2-Subnetz Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind. `requiredTagKeys` Die Steuerung schlägt fehl, wenn das Subnetz keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Subnetz mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2-Subnetz finden Sie unter Taggen Ihrer Amazon EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.45] EC2-Volumes sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::Subnet`

AWS Config Regel: `tagged-ec2-subnet` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EC2 EC2-Volume Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn das Volume keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Volume mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2-Volume finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.46] Amazon VPCs sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::VPC`

AWS Config Regel: `tagged-ec2-vpc` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon Virtual Private Cloud (Amazon VPC) Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Amazon VPC keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Amazon VPC mit keinem Schlüssel gekennzeichnet ist. System-Tags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer VPC finden Sie unter Taggen Ihrer Amazon EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.47] Amazon VPC Endpoint Services sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::VPCEndpointService`

AWS Config Regel: `tagged-ec2-vpcendpointservice` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon VPC-Endpunktservice über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Endpunkt-Service keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Endpunktdienst mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon VPC-Endpunktservice finden Sie unter Tags verwalten im Abschnitt Konfiguration eines Endpunktdienstes des AWS PrivateLink Handbuchs.

[EC2.48] Amazon VPC-Flow-Logs sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::FlowLog`

AWS Config Regel: `tagged-ec2-flowlog` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon VPC-Flow-Log Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn das Flow-Protokoll keine Tag-Schlüssel enthält oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Flow-Protokoll mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon VPC-Flow-Protokoll finden Sie unter Taggen eines Flow-Protokolls im Amazon VPC-Benutzerhandbuch.

[EC2.49] Amazon VPC-Peering-Verbindungen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::VPCPeeringConnection`

AWS Config Regel: `tagged-ec2-vpcpeeringconnection` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList	Liste der Tags, die die AWS	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen	

Dieses Steuerelement prüft, ob eine Amazon VPC-Peering-Verbindung Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind. `requiredTagKeys` Die Steuerung schlägt fehl, wenn die Peering-Verbindung keine Tag-Schlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Peering-Verbindung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Amazon VPC-Peering-Verbindung finden Sie unter Taggen Ihrer Amazon EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.50] EC2-VPN-Gateways sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::VPNGateway`

AWS Config Regel: `tagged-ec2-vpngateway` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EC2 EC2-VPN-Gateway über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn das VPN-Gateway keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das VPN-Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2-VPN-Gateway finden Sie unter Taggen Ihrer Amazon EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (12), NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIst.800-53.R5 AU-10, NIst.800-53.R5 AU-2, NIST.800-53.R5 AU-2 800-53.R5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 AU-9 (7), NIST.800-53.R5 CA-7, NIst.800-53.R5 SC-7 (9), NIst.800-53.R5 SI-3 (8), NIst.800-53.R5 SI-4, NIST.800-53,R5 SI-4 (20), NIST.800-53,R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::ClientVpnEndpoint`

AWS Config Regel: **`ec2-client-vpn-connection-log-enabled`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen AWS Client VPN Endpunkt die Client-Verbindungsprotokollierung aktiviert ist. Die Steuerung schlägt fehl, wenn für den Endpunkt die Client-Verbindungsprotokollierung nicht aktiviert ist.

Client-VPN-Endpunkte ermöglichen Remote-Clients die sichere Verbindung zu Ressourcen in einer Virtual Private Cloud (VPC) in. AWS Verbindungsprotokolle ermöglichen es Ihnen, Benutzeraktivitäten auf dem VPN-Endpunkt zu verfolgen und bieten Transparenz. Wenn Sie die Verbindungsprotokollierung aktivieren, können Sie den Namen eines Protokolldatenstroms in der Protokollgruppe angeben. Wenn Sie keinen Protokollstream angeben, erstellt der Client-VPN-Dienst einen für Sie.

Abhilfe

Informationen zum Aktivieren der Verbindungsprotokollierung finden Sie unter Aktivieren der Verbindungsprotokollierung für einen vorhandenen Client-VPN-Endpunkt im AWS Client VPN Administratorhandbuch.

[EC2.52] EC2-Transit-Gateways sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EC2::TransitGateway`

AWS Config Regel: `tagged-ec2-transitgateway` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein Amazon EC2-Transit-Gateway Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Kontrolle schlägt fehl, wenn das Transit-Gateway keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Transit-Gateway mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EC2-Transit-Gateway finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 zu Remote-Serververwaltungsports zulassen

Verwandte Anforderungen: CIS Foundations Benchmark v3.0.0/5.2 AWS

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Konfiguration von Sicherheitsgruppen

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::SecurityGroup`

AWS Config -Regel: `vpc-sg-port-restriction-check`

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`ipType`	Die IP-Version	String	Nicht anpassbar	`IPv4`
`restrictPorts`	Liste der Ports, die eingehenden Datenverkehr ablehnen sollen	IntegerList	Nicht anpassbar	`22,3389`

Diese Steuerung prüft, ob eine Amazon EC2-Sicherheitsgruppe den Zugriff von 0.0.0.0/0 zu den Remote-Serververwaltungsports (Ports 22 und 3389) zulässt. Die Kontrolle schlägt fehl, wenn die Sicherheitsgruppe den Zugriff von 0.0.0.0/0 zu Port 22 oder 3389 zulässt.

Sicherheitsgruppen bieten eine statusabhängige Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen. AWS Es wird empfohlen, dass keine Sicherheitsgruppe uneingeschränkten Zugriff auf Ports für die Remoteserververwaltung zulässt, z. B. SSH zu Port 22 und RDP zu Port 3389, wobei entweder die Protokolle TDP (6), UDP (17) oder ALL (-1) verwendet werden. Wenn der öffentliche Zugriff auf diese Ports zugelassen wird, erhöht sich die Angriffsfläche für Ressourcen und das Risiko einer Beeinträchtigung der Ressourcen.

Abhilfe

Informationen zum Aktualisieren einer EC2-Sicherheitsgruppenregel, um eingehenden Datenverkehr zu den angegebenen Ports zu verhindern, finden Sie unter Sicherheitsgruppenregeln aktualisieren im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances. Nachdem Sie in der Amazon EC2 EC2-Konsole eine Sicherheitsgruppe ausgewählt haben, wählen Sie Aktionen, Regeln für eingehenden Datenverkehr bearbeiten. Entfernen Sie die Regel, die den Zugriff auf Port 22 oder Port 3389 ermöglicht.

[EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugang von: :/0 zu Remote-Serveradministrationsports zulassen

Verwandte Anforderungen: CIS Foundations Benchmark v3.0.0/5.3 AWS

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Konfiguration von Sicherheitsgruppen

Schweregrad: Hoch

Art der Ressource: `AWS::EC2::SecurityGroup`

AWS Config -Regel: `vpc-sg-port-restriction-check`

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`ipType`	Die IP-Version	String	Nicht anpassbar	`IPv6`
`restrictPorts`	Liste der Ports, die eingehenden Datenverkehr ablehnen sollen	IntegerList	Nicht anpassbar	`22,3389`

Dieses Steuerelement prüft, ob eine Amazon EC2-Sicherheitsgruppe den Zugriff von: :/0 zu den Remote-Serververwaltungsports (Ports 22 und 3389) zulässt. Die Kontrolle schlägt fehl, wenn die Sicherheitsgruppe den Zugang von: :/0 zu Port 22 oder 3389 zulässt.

Sicherheitsgruppen bieten eine statusabhängige Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen. AWS Es wird empfohlen, dass keine Sicherheitsgruppe uneingeschränkten Zugriff auf Ports für die Remoteserververwaltung zulässt, z. B. SSH zu Port 22 und RDP zu Port 3389, wobei entweder die Protokolle TDP (6), UDP (17) oder ALL (-1) verwendet werden. Wenn der öffentliche Zugriff auf diese Ports zugelassen wird, erhöht sich die Angriffsfläche für Ressourcen und das Risiko einer Beeinträchtigung der Ressourcen.

Abhilfe

Informationen zum Aktualisieren einer EC2-Sicherheitsgruppenregel, um eingehenden Datenverkehr zu den angegebenen Ports zu verhindern, finden Sie unter Sicherheitsgruppenregeln aktualisieren im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances. Nachdem Sie in der Amazon EC2 EC2-Konsole eine Sicherheitsgruppe ausgewählt haben, wählen Sie Aktionen, Regeln für eingehenden Datenverkehr bearbeiten. Entfernen Sie die Regel, die den Zugriff auf Port 22 oder Port 3389 ermöglicht.

Amazon EC2 Auto Scaling-Steuerelemente

Diese Kontrollen beziehen sich auf Amazon EC2 Auto Scaling Scaling-Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden

Verwandte Anforderungen: PCI DSS v3.2.1/2.2, NIST.800-53.R5 CA-7, NIST.800-53.R5 CP-2 (2), NIst.800-53.R5 SI-2

Kategorie: Identifizieren > Bestand

Schweregrad: Niedrig

Art der Ressource: `AWS::AutoScaling::AutoScalingGroup`

AWS Config -Regel: `autoscaling-group-elb-healthcheck-required`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe, die einem Load Balancer zugeordnet ist, Elastic Load Balancing (ELB) -Zustandsprüfungen verwendet. Die Steuerung schlägt fehl, wenn die Auto Scaling Scaling-Gruppe keine ELB-Zustandsprüfungen verwendet.

ELB-Zustandsprüfungen stellen sicher, dass eine Auto Scaling Scaling-Gruppe den Zustand einer Instance anhand zusätzlicher Tests ermitteln kann, die vom Load Balancer bereitgestellt werden. Die Verwendung von Elastic Load Balancing Health Checks trägt auch dazu bei, die Verfügbarkeit von Anwendungen zu unterstützen, die EC2 Auto Scaling Scaling-Gruppen verwenden.

Abhilfe

Informationen zum Hinzufügen von Elastic Load Balancing Balancing-Zustandsprüfungen finden Sie unter Elastic Load Balancing Balancing-Zustandsprüfungen hinzufügen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

[AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-2 (2), NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::AutoScaling::AutoScalingGroup`

AWS Config -Regel: `autoscaling-multiple-az`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`minAvailabilityZones`	Mindestanzahl von Availability Zones	Enum	`2, 3, 4, 5, 6`	`2`

Dieses Steuerelement prüft, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe mindestens die angegebene Anzahl von Availability Zones (AZs) umfasst. Die Steuerung schlägt fehl, wenn eine Auto Scaling Scaling-Gruppe nicht mindestens die angegebene Anzahl von AZs umfasst. Sofern Sie keinen benutzerdefinierten Parameterwert für die Mindestanzahl von AZs angeben, verwendet Security Hub einen Standardwert von zwei AZs.

Eine Auto Scaling Scaling-Gruppe, die sich nicht über mehrere AZs erstreckt, kann keine Instances in einer anderen AZ starten, um dies zu kompensieren, wenn die konfigurierte einzelne AZ nicht mehr verfügbar ist. In einigen Anwendungsfällen kann jedoch eine Auto Scaling Scaling-Gruppe mit einer einzigen Availability Zone bevorzugt werden, z. B. bei Batch-Jobs oder wenn die Inter-AZ-Übertragungskosten auf ein Minimum beschränkt werden müssen. In solchen Fällen können Sie diese Steuerung deaktivieren oder ihre Ergebnisse unterdrücken.

Abhilfe

Informationen zum Hinzufügen von AZs zu einer vorhandenen Auto Scaling Scaling-Gruppe finden Sie unter Availability Zones hinzufügen und entfernen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

[AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen

Verwandte Anforderungen: NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-6, NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Ressourcentyp: `AWS::AutoScaling::LaunchConfiguration`

AWS Config -Regel: `autoscaling-launchconfig-requires-imdsv2`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob IMDSv2 auf allen Instances aktiviert ist, die von Amazon EC2 Auto Scaling Scaling-Gruppen gestartet wurden. Die Steuerung schlägt fehl, wenn die Version des Instance Metadata Service (IMDS) nicht in der Startkonfiguration enthalten ist oder wenn sowohl IMDSv1 als auch IMDSv2 aktiviert sind.

IMDS stellt Daten über Ihre Instance bereit, die Sie verwenden können, um die laufende Instance zu konfigurieren oder zu verwalten.

Version 2 des IMDS fügt neue Schutzmaßnahmen hinzu, die in IMDSv1 nicht verfügbar waren, um Ihre EC2-Instances weiter zu schützen.

Abhilfe

Eine Auto Scaling Scaling-Gruppe ist jeweils einer Startkonfiguration zugeordnet. Sie können eine Startkonfiguration nicht ändern, nachdem Sie sie erstellt haben. Um die Startkonfiguration für eine Auto Scaling Scaling-Gruppe zu ändern, verwenden Sie eine bestehende Startkonfiguration als Grundlage für eine neue Startkonfiguration mit aktiviertem IMDSv2. Weitere Informationen finden Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[AutoScaling.4] Die Auto Scaling Scaling-Gruppenstartkonfiguration sollte kein Metadaten-Response-Hop-Limit größer als 1 haben

> **Important**
>
> Security Hub hat diese Kontrolle im April 2024 eingestellt. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::AutoScaling::LaunchConfiguration`

AWS Config -Regel: `autoscaling-launch-config-hop-limit`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement überprüft die Anzahl der Netzwerk-Hops, die ein Metadaten-Token zurücklegen kann. Die Steuerung schlägt fehl, wenn das Limit für Metadaten-Antwort-Hops größer als ist1.

Der Instance Metadata Service (IMDS) stellt Metadateninformationen zu einer Amazon EC2 EC2-Instance bereit und ist für die Anwendungskonfiguration nützlich. Die Beschränkung der PUT HTTP-Antwort für den Metadaten-Service auf die EC2-Instance schützt das IMDS vor unbefugter Nutzung.

Das TTL-Feld (Time To Live) im IP-Paket wird bei jedem Hop um eins reduziert. Diese Reduzierung kann verwendet werden, um sicherzustellen, dass das Paket nicht außerhalb von EC2 übertragen wird. IMDSv2 schützt EC2-Instances, die möglicherweise als offene Router, Layer-3-Firewalls, VPNs, Tunnel oder NAT-Geräte falsch konfiguriert wurden, wodurch verhindert wird, dass unbefugte Benutzer Metadaten abrufen. Mit IMDSv2 kann die PUT Antwort, die das geheime Token enthält, nicht außerhalb der Instance übertragen werden, da das standardmäßige Hop-Limit für die Beantwortung von Metadaten auf festgelegt ist. 1 Wenn dieser Wert jedoch größer als ist1, kann das Token die EC2-Instance verlassen.

Abhilfe

Informationen zum Ändern des Metadaten-Response-Hop-Limits für eine bestehende Startkonfiguration finden Sie unter Ändern von Instance-Metadatenoptionen für bestehende Instances im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

[Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben

Verwandte Anforderungen: NIST.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::AutoScaling::LaunchConfiguration`

AWS Config -Regel: `autoscaling-launch-config-public-ip-disabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die zugehörige Startkonfiguration einer Auto Scaling Scaling-Gruppe den Instances der Gruppe eine öffentliche IP-Adresse zuweist. Die Steuerung schlägt fehl, wenn die zugehörige Startkonfiguration eine öffentliche IP-Adresse zuweist.

Amazon EC2 EC2-Instances in einer Auto Scaling Scaling-Gruppenstartkonfiguration sollten keine zugeordnete öffentliche IP-Adresse haben, außer in begrenzten Randfällen. Amazon EC2 EC2-Instances sollten nur hinter einem Load Balancer zugänglich sein, anstatt direkt dem Internet ausgesetzt zu sein.

Abhilfe

Eine Auto Scaling Scaling-Gruppe ist jeweils einer Startkonfiguration zugeordnet. Sie können eine Startkonfiguration nicht ändern, nachdem Sie sie erstellt haben. Um die Startkonfiguration einer

Auto-Scaling-Gruppe zu ändern, verwenden Sie eine vorhandene Startkonfiguration als Grundlage für eine neue Startkonfiguration. Aktualisieren Sie dann die Auto-Scaling-Gruppe so, dass die neue Startkonfiguration verwendet wird. step-by-step Anweisungen finden Sie unter Ändern der Startkonfiguration für eine Auto Scaling Scaling-Gruppe im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch. Wählen Sie bei der Erstellung der neuen Startkonfiguration unter Zusätzliche Konfiguration für Erweiterte Details und IP-Adresstyp die Option Keinen Instances eine öffentliche IP-Adresse zuweisen aus.

Nachdem Sie die Startkonfiguration geändert haben, startet Auto Scaling neue Instances mit den neuen Konfigurationsoptionen. Bestehende Instanzen sind nicht betroffen. Um eine bestehende Instance zu aktualisieren, empfehlen wir Ihnen, Ihre Instance zu aktualisieren oder die automatische Skalierung zuzulassen, um ältere Instances auf der Grundlage Ihrer Kündigungsrichtlinien schrittweise durch neuere Instances zu ersetzen. Weitere Informationen zur Aktualisierung von Auto Scaling Scaling-Instances finden Sie unter Auto Scaling Scaling-Instances aktualisieren im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

[AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-2 (2), NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::AutoScaling::AutoScalingGroup`

AWS Config -Regel: `autoscaling-multiple-instance-types`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe mehrere Instance-Typen verwendet. Die Steuerung schlägt fehl, wenn für die Auto Scaling Scaling-Gruppe nur ein Instanztyp definiert ist.

Sie können die Verfügbarkeit verbessern, indem Sie Ihre Anwendung auf mehreren Instance-Typen bereitstellen, die in mehreren Availability Zones ausgeführt werden. Security Hub empfiehlt die Verwendung mehrerer Instanztypen, damit die Auto Scaling Scaling-Gruppe einen anderen Instance-

Typ starten kann, wenn die Instance-Kapazität in den von Ihnen ausgewählten Availability Zones nicht ausreicht.

Abhilfe

Informationen zum Erstellen einer Auto Scaling Scaling-Gruppe mit mehreren Instance-Typen finden Sie unter Auto Scaling Scaling-Gruppen mit mehreren Instance-Typen und Kaufoptionen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

[AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.r5 CM-2 (2)

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::AutoScaling::AutoScalingGroup`

AWS Config -Regel: `autoscaling-launch-template`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe anhand einer EC2-Startvorlage erstellt wurde. Diese Steuerung schlägt fehl, wenn eine Amazon EC2 Auto Scaling Scaling-Gruppe nicht mit einer Startvorlage erstellt wird oder wenn keine Startvorlage in einer Richtlinie für gemischte Instanzen angegeben ist.

Eine EC2 Auto Scaling Scaling-Gruppe kann entweder aus einer EC2-Startvorlage oder einer Startkonfiguration erstellt werden. Die Verwendung einer Startvorlage zur Erstellung einer Auto Scaling Scaling-Gruppe stellt jedoch sicher, dass Sie Zugriff auf die neuesten Funktionen und Verbesserungen haben.

Abhilfe

Informationen zum Erstellen einer Auto Scaling Scaling-Gruppe mit einer EC2-Startvorlage finden Sie unter Erstellen einer Auto Scaling Scaling-Gruppe mithilfe einer Startvorlage im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch. Informationen zum Ersetzen einer Startkonfiguration durch eine

Startvorlage finden Sie unter Ersetzen einer Startkonfiguration durch eine Startvorlage im Amazon EC2 EC2-Benutzerhandbuch für Windows-Instances.

[AutoScaling.10] EC2 Auto Scaling Scaling-Gruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AutoScaling::AutoScalingGroup`

AWS Config Regel: `tagged-autoscaling-autoscalinggroup` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Auto Scaling Scaling-Gruppe keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Auto Scaling Scaling-Gruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Auto Scaling Scaling-Gruppe finden Sie unter Tag Auto Scaling Scaling-Gruppen und -Instances im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Amazon EC2 Systems Manager Manager-Steuerelemente

Diese Kontrollen beziehen sich auf Amazon EC2 EC2-Instances, die von AWS Systems Manager verwaltet werden.

Diese Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager

Verwandte Anforderungen: PCI DSS v3.2.1/2.4, NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2), NIST.800-53.R5 CM-8, NIST.800-53.R5 CM-8 (1), NIST.800-53.r5 CM-8 (2), NIST.800-53.R5 CM-8 (3), NIST.800-53.R5 SA-15 (2), NIST.800-53.R5 SA-15 (8), NIST.800-53.R5 SA-3, NIST.800-53.R5 SI-2 (3)

Kategorie: Identifizieren > Bestand

Schweregrad: Mittel

Evaluierte Ressource: `AWS::EC2::Instance`

Erforderliche AWS Config Aufzeichnungsressourcen:`AWS::EC2::Instance`, `AWS::SSM::ManagedInstanceInventory`

AWS Config -Regel: `ec2-instance-managed-by-systems-manager`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die gestoppten und laufenden EC2-Instances in Ihrem Konto von AWS Systems Manager verwaltet werden. Systems Manager ist ein AWS-Service Programm, mit dem Sie Ihre AWS Infrastruktur anzeigen und steuern können.

Um Sie bei der Aufrechterhaltung von Sicherheit und Compliance zu unterstützen, scannt Systems Manager Ihre gestoppten und laufenden verwalteten Instances. Eine verwaltete Instanz ist eine Maschine, die für die Verwendung mit Systems Manager konfiguriert ist. Systems Manager meldet dann alle festgestellten Richtlinienverstöße oder ergreift Korrekturmaßnahmen. Systems Manager hilft Ihnen auch bei der Konfiguration und Wartung Ihrer verwalteten Instanzen.

Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch.

Abhilfe

Informationen zur Verwaltung von EC2-Instances mit Systems Manager finden Sie unter Amazon EC2 EC2-Hostverwaltung im AWS Systems Manager Benutzerhandbuch. Im Abschnitt Konfigurationsoptionen können Sie die Standardoptionen beibehalten oder sie nach Bedarf für Ihre bevorzugte Konfiguration ändern.

[SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben

Verwandte Anforderungen: PCI DSS v3.2.1/6.2, NIST.800-53.R5 CM-8 (3), NIST.800-53.R5 SI-2, NIst.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (3), NIST.800-53.R5 SI-2 (4), NIst.800-53.R5 SI-2 (5)

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: `AWS::SSM::PatchCompliance`

AWS Config -Regel: `ec2-managedinstance-patch-compliance-status-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement überprüft, ob der Konformitätsstatus von Systems Manager Patch Compliance `COMPLIANT` oder `NON_COMPLIANT` nach der Patch-Installation auf der Instanz ist. Die Kontrolle schlägt fehl, wenn der Konformitätsstatus lautet`NON_COMPLIANT`. Das Steuerelement überprüft nur Instanzen, die von Systems Manager Patch Manager verwaltet werden.

Durch das Patchen Ihrer EC2-Instances gemäß den Anforderungen Ihres Unternehmens wird die Angriffsfläche Ihrer Instances reduziert. AWS-Konten

Abhilfe

Systems Manager empfiehlt die Verwendung von Patch-Richtlinien, um das Patchen für Ihre verwalteten Instanzen zu konfigurieren. Sie können auch Systems Manager Manager-Dokumente verwenden, wie im folgenden Verfahren beschrieben, um eine Instanz zu patchen.

So korrigieren Sie nicht konforme Patches

1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie für Node Management die Option Run Command und anschließend Run Command aus.
3. Wählen Sie die Option für AWS- RunPatchBaseline.
4. Ändern Sie die Operation in Install (Installieren).

5. Wählen Sie Instanzen manuell auswählen und wählen Sie dann die nicht konformen Instanzen aus.
6. Wählen Sie Ausführen aus.
7. Wenn der Befehl abgeschlossen ist, wählen Sie im Navigationsbereich Compliance aus, um den neuen Compliance-Status Ihrer gepatchten Instances zu überwachen.

[SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben

Verwandte Anforderungen: PCI DSS v3.2.1/2.4, NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2), NIST.800-53.R5 CM-8, NIST.800-53.R5 CM-8 (1), NIST.800-53.r5 CM-8 (3), NIST.800-53.R5 SI-2 (3)

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Art der Ressource: `AWS::SSM::AssociationCompliance`

AWS Config -Regel: `ec2-managedinstance-association-compliance-status-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Mit diesem Steuerelement wird geprüft, ob der Status der AWS Systems Manager Zuordnung auf einer Instanz den Status „Konformität“ hat `COMPLIANT` oder `NON_COMPLIANT` nachdem die Zuordnung ausgeführt wurde. Die Kontrolle schlägt fehl, wenn der Compliance-Status der Assoziation lautet`NON_COMPLIANT`.

Eine State Manager-Zuordnung ist eine Konfiguration, die Ihren verwalteten Instances zugewiesen ist. Die Konfiguration definiert den Status, den Sie auf Ihren Instances beibehalten möchten. Eine Zuordnung kann beispielsweise angeben, dass Antivirensoftware auf Ihren Instanzen installiert und ausgeführt werden muss oder dass bestimmte Ports geschlossen sein müssen.

Nachdem Sie eine oder mehrere State Manager-Zuordnungen erstellt haben, stehen Ihnen die Informationen zum Compliance-Status sofort zur Verfügung. Sie können den Konformitätsstatus in der Konsole oder als Reaktion auf AWS CLI Befehle oder entsprechende Systems Manager

API-Aktionen anzeigen. Bei Zuordnungen zeigt Configuration Compliance den Konformitätsstatus (`Compliant`oder`Non-compliant`) an. Außerdem wird der Schweregrad angezeigt, der der Zuordnung zugewiesen wurde, z. B. `Critical` oder`Medium`.

Weitere Informationen zur Einhaltung der State Manager-Zuordnungen finden Sie im AWS Systems Manager Benutzerhandbuch unter Informationen zur Einhaltung von State Manager-Zuordnungen.

Abhilfe

Eine fehlgeschlagene Zuordnung kann auf verschiedene Dinge zurückzuführen sein, z. B. auf Ziele und SSM-Dokumentnamen. Um dieses Problem zu beheben, müssen Sie zunächst die Zuordnung identifizieren und untersuchen, indem Sie sich den Zuordnungsverlauf ansehen. Anweisungen zum Anzeigen des Zuordnungsverlaufs finden Sie unter Zuordnungshistorien anzeigen im AWS Systems Manager Benutzerhandbuch.

Nach der Untersuchung können Sie die Zuordnung bearbeiten, um das festgestellte Problem zu beheben. Sie können eine Zuordnung bearbeiten, um den Namen, den Zeitplan, den Schweregrad oder die Ziele zu ändern. Nachdem Sie eine Zuordnung bearbeitet haben, AWS Systems Manager wird eine neue Version erstellt. Anweisungen zum Bearbeiten einer Zuordnung finden Sie im AWS Systems Manager Benutzerhandbuch unter Bearbeiten und Erstellen einer neuen Version einer Zuordnung.

[SSM.4] SSM-Dokumente sollten nicht öffentlich sein

Verwandte Anforderungen: NIST.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Kritisch

Art der Ressource: `AWS::SSM::Document`

AWS Config -Regel: `ssm-document-not-public`

Art des Zeitplans: Periodisch

Parameter: Keine

Mit dieser Kontrolle wird geprüft, ob AWS Systems Manager Dokumente, die dem Konto gehören, öffentlich sind. Diese Kontrolle schlägt fehl, wenn SSM-Dokumente mit dem Eigentümer öffentlich `Self` sind.

Öffentliche SSM-Dokumente ermöglichen möglicherweise unbeabsichtigten Zugriff auf Ihre Dokumente. Ein öffentliches SSM-Dokument kann wertvolle Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Sofern Ihr Anwendungsfall die öffentliche Freigabe nicht erfordert, empfehlen wir, die Einstellung für die öffentliche Freigabe für Systems Manager Manager-Dokumente zu blockieren, die Eigentum von sind`Self`.

Abhilfe

Informationen zum Blockieren der öffentlichen Freigabe von SSM-Dokumenten finden Sie unter Sperren der öffentlichen Freigabe von SSM-Dokumenten im AWS Systems Manager Benutzerhandbuch.

Steuerelemente für das Amazon Elastic File System

Diese Kontrollen beziehen sich auf Amazon EFS-Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/2.4.1, NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIst.800-53.R5 SC-28 (1), NIst.800-53.R5 SC-7 (10), NIst.800-53,5r5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::EFS::FileSystem`

AWS Config -Regel: `efs-encrypted-check`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon Elastic File System so konfiguriert ist, dass es die Dateidaten verschlüsselt mit AWS KMS. Die Prüfung schlägt in den folgenden Fällen fehl.

- `Encrypted`ist `false` in der `DescribeFileSystems`Antwort auf eingestellt.
- Der `KmsKeyId`-Schlüssel in der `DescribeFileSystems`-Antwort stimmt nicht mit dem `KmsKeyId`-Parameter für `efs-encrypted-check` überein.

Beachten Sie, dass dieses Steuerelement den `KmsKeyId`-Parameter nicht für `efs-encrypted-check` verwendet. Es überprüft nur den Wert von `Encrypted`.

Für eine zusätzliche Sicherheitsebene für Ihre sensiblen Daten in Amazon EFS sollten Sie verschlüsselte Dateisysteme erstellen. Amazon EFS unterstützt die Verschlüsselung von Dateisystemen im Ruhezustand. Sie können die Verschlüsselung von Daten im Ruhezustand aktivieren, wenn Sie ein Amazon EFS-Dateisystem erstellen. Weitere Informationen zur Amazon EFS-Verschlüsselung finden Sie unter Datenverschlüsselung in Amazon EFS im Amazon Elastic File System-Benutzerhandbuch.

Abhilfe

Einzelheiten zur Verschlüsselung eines neuen Amazon EFS-Dateisystems finden Sie unter Verschlüsseln ruhender Daten im Amazon Elastic File System-Benutzerhandbuch.

[EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6, NIST.800-53.R5 CP-6 (1), NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 CP-9, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Resilienz > Backup

Schweregrad: Mittel

Art der Ressource: `AWS::EFS::FileSystem`

AWS Config -Regel: `efs-in-backup-plan`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon Elastic File System (Amazon EFS) -Dateisysteme zu den Sicherungsplänen in hinzugefügt wurden AWS Backup. Die Kontrolle schlägt fehl, wenn Amazon EFS-Dateisysteme nicht in den Backup-Plänen enthalten sind.

Die Einbeziehung von EFS-Dateisystemen in die Backup-Pläne hilft Ihnen, Ihre Daten vor Löschung und Datenverlust zu schützen.

Abhilfe

Informationen zum Aktivieren automatischer Backups für ein vorhandenes Amazon EFS-Dateisystem finden Sie unter Erste Schritte 4: Automatische Amazon EFS-Backups erstellen im AWS Backup Entwicklerhandbuch.

[EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen

Verwandte Anforderungen: NIST.800-53.R5 AC-6 (10)

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::EFS::AccessPoint`

AWS Config -Regel: `efs-access-point-enforce-root-directory`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob Amazon EFS-Zugriffspunkte so konfiguriert sind, dass sie ein Stammverzeichnis erzwingen. Die Steuerung schlägt fehl, wenn der `Path` Wert von auf `/` (das Standard-Stammverzeichnis des Dateisystems) gesetzt ist.

Wenn Sie ein Stammverzeichnis erzwingen, verwendet der NFS-Client, der den Zugriffspunkt verwendet, das auf dem Zugriffspunkt konfigurierte Stammverzeichnis anstelle des Stammverzeichnisses des Dateisystems. Durch die Festlegung eines Stammverzeichnisses für einen

Access Point wird der Datenzugriff eingeschränkt, da sichergestellt wird, dass Benutzer des Access Points nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.

Abhilfe

Anweisungen zum Erzwingen eines Stammverzeichnisses für einen Amazon EFS-Zugriffspunkt finden Sie unter Erzwingen eines Stammverzeichnisses mit einem Zugriffspunkt im Amazon Elastic File System-Benutzerhandbuch.

[EFS.4] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen

Verwandte Anforderungen: NIST.800-53.R5 AC-6 (2)

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::EFS::AccessPoint`

AWS Config -Regel: `efs-access-point-enforce-user-identity`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob Amazon EFS Access Points so konfiguriert sind, dass sie eine Benutzeridentität erzwingen. Diese Steuerung schlägt fehl, wenn beim Erstellen des EFS-Zugriffspunkts keine POSIX-Benutzeridentität definiert wurde.

Amazon-EFS-Zugangspunkte sind anwendungsspezifische Einstiegspunkte in ein EFS-Dateisystem, die das Verwalten des Anwendungszugriffs auf freigegebene Datensätze erleichtern. Zugriffspunkte können eine Benutzeridentität, einschließlich der POSIX-Gruppen des Benutzers, für alle Dateisystemanforderungen erzwingen, die über den Zugriffspunkt erfolgen. Zugriffspunkte können auch ein anderes Stammverzeichnis für das Dateisystem erzwingen, so dass Clients nur auf Daten im angegebenen Verzeichnis oder in seinen Unterverzeichnissen zugreifen können.

Abhilfe

Informationen zur Durchsetzung einer Benutzeridentität für einen Amazon EFS Access Point finden Sie unter Durchsetzung einer Benutzeridentität mithilfe eines Access Points im Amazon Elastic File System-Benutzerhandbuch.

[EFS.5] EFS-Zugangspunkte sollten markiert werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::EFS::AccessPoint`

AWS Config Regel: `tagged-efs-accesspoint` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EFS-Zugriffspunkt über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind`requiredTagKeys`. Die Kontrolle schlägt fehl, wenn der Access Point keine Tag-Schlüssel hat oder wenn er nicht über alle im Parameter angegebenen Schlüssel verfügt`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft die Steuerung nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Access Point mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern

verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EFS-Zugangspunkt finden Sie unter Tagging Amazon EFS-Ressourcen im Amazon Elastic File System-Benutzerhandbuch.

[EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Mittel

Art der Ressource: `AWS::EFS::FileSystem`

AWS Config -Regel: `efs-mount-target-public-accessible`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon EFS-Mount-Ziel einem privaten Subnetz zugeordnet ist. Die Steuerung schlägt fehl, wenn das Mount-Ziel einem öffentlichen Subnetz zugeordnet ist.

Standardmäßig ist ein Dateisystem nur von der Virtual Private Cloud (VPC) aus zugänglich, in der Sie es erstellt haben. Wir empfehlen, EFS-Mount-Ziele in privaten Subnetzen zu erstellen, auf die nicht

über das Internet zugegriffen werden kann. Dadurch wird sichergestellt, dass Ihr Dateisystem nur autorisierten Benutzern zugänglich ist und nicht für unbefugten Zugriff oder Angriffe anfällig ist.

Abhilfe

Sie können die Zuordnung zwischen einem EFS-Mount-Ziel und einem Subnetz nicht ändern, nachdem Sie das Mount-Ziel erstellt haben. Um ein vorhandenes Mount-Ziel einem anderen Subnetz zuzuordnen, müssen Sie ein neues Mount-Ziel in einem privaten Subnetz erstellen und dann das alte Mount-Ziel entfernen. Informationen zur Verwaltung von Mount-Zielen finden Sie unter Erstellen und Verwalten von Mount-Zielen und Sicherheitsgruppen im Amazon Elastic File System-Benutzerhandbuch.

Steuerelemente für Amazon Elastic Kubernetes Service

Diese Kontrollen beziehen sich auf Amazon EKS-Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein

Verwandte Anforderungen: NIST.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schützen > Sicheres Zugriffsmanagement > Ressource nicht öffentlich zugänglich

Schweregrad: Hoch

Art der Ressource: `AWS::EKS::Cluster`

AWS Config -Regel: `eks-endpoint-no-public-access`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon EKS-Cluster-Endpunkt öffentlich zugänglich ist. Die Kontrolle schlägt fehl, wenn ein EKS-Cluster über einen öffentlich zugänglichen Endpunkt verfügt.

Wenn Sie einen neuen Cluster erstellen, erstellt Amazon EKS einen Endpunkt für den verwalteten Kubernetes-API-Server, den Sie für die Kommunikation mit Ihrem Cluster verwenden. Standardmäßig ist dieser API-Server-Endpunkt öffentlich im Internet verfügbar. Der Zugriff auf den API-Server wird durch eine Kombination aus AWS Identity and Access Management (IAM) und nativer Kubernetes-Rollenbasierter Zugriffskontrolle (RBAC) gesichert. Indem Sie den öffentlichen Zugriff auf den Endpunkt unterbinden, können Sie verhindern, dass Ihr Cluster unbeabsichtigt gefährdet ist und Sie darauf zugreifen können.

Abhilfe

Informationen zum Ändern des Endpunktzugriffs für einen vorhandenen EKS-Cluster finden Sie unter Ändern des Cluster-Endpunktzugriffs im Amazon EKS-Benutzerhandbuch. Sie können den Endpunktzugriff für einen neuen EKS-Cluster einrichten, wenn Sie ihn erstellen. Anweisungen zum Erstellen eines neuen Amazon EKS-Clusters finden Sie unter Erstellen eines Amazon EKS-Clusters im Amazon EKS-Benutzerhandbuch.

[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 SI-2, NIst.800-53.R5 SI-2 (2), NIst.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5)

Kategorie: Identifizieren > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::EKS::Cluster`

AWS Config -Regel: `eks-cluster-supported-version`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `oldestVersionSupported`: `1.26` (nicht anpassbar)

Dieses Steuerelement prüft, ob ein Amazon Elastic Kubernetes Service (Amazon EKS-Cluster) auf einer unterstützten Kubernetes-Version ausgeführt wird. Die Steuerung schlägt fehl, wenn der EKS-Cluster auf einer nicht unterstützten Version ausgeführt wird.

Wenn Ihre Anwendung keine bestimmte Version von Kubernetes benötigt, empfehlen wir Ihnen, die neueste verfügbare Kubernetes-Version zu verwenden, die von EKS für Ihre Cluster unterstützt wird. Weitere Informationen finden Sie im Amazon EKS Kubernetes-Veröffentlichungskalender und unter Amazon EKS-Versionsunterstützung und häufig gestellte Fragen im Amazon EKS-Benutzerhandbuch.

Abhilfe

Informationen zum Aktualisieren eines EKS-Clusters finden Sie unter Aktualisieren einer Amazon EKS-Cluster-Kubernetes-Version im Amazon EKS-Benutzerhandbuch.

[EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden

Verwandte Anforderungen: NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-12, NIST.800-53.R5 SC-13, NIST.800-53.R5 SI-28

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::EKS::Cluster`

AWS Config -Regel: `eks-secrets-encrypted`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon EKS-Cluster verschlüsselte Kubernetes-Geheimnisse verwendet. Die Steuerung schlägt fehl, wenn die Kubernetes-Geheimnisse des Clusters nicht verschlüsselt sind.

Wenn Sie Geheimnisse verschlüsseln, können Sie AWS Key Management Service (AWS KMS) -Schlüssel verwenden, um die in etcd für Ihren Cluster gespeicherten Kubernetes-Geheimnisse mit Umschlägen zu verschlüsseln. Diese Verschlüsselung erfolgt zusätzlich zur EBS-Volumenverschlüsselung, die standardmäßig für alle Daten (einschließlich Secrets) aktiviert ist, die in etcd als Teil eines EKS-Clusters gespeichert sind. Durch die Verschlüsselung von Geheimnissen für Ihren EKS-Cluster können Sie eine umfassende Verteidigungsstrategie für Kubernetes-Anwendungen implementieren, indem Sie Kubernetes-Geheimnisse mit einem KMS-Schlüssel verschlüsseln, den Sie definieren und verwalten.

Abhilfe

Informationen zum Aktivieren der Geheimverschlüsselung auf einem EKS-Cluster finden Sie unter Enabling Secret Encryption on a existing cluster im Amazon EKS-Benutzerhandbuch.

[EKS.6] EKS-Cluster sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EKS::Cluster`

AWS Config Regel: `tagged-eks-cluster` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon EKS-Cluster Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Cluster keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Cluster mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EKS-Cluster finden Sie unter Taggen Ihrer Amazon EKS-Ressourcen im Amazon EKS-Benutzerhandbuch.

[EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::EKS::IdentityProviderConfig`

AWS Config Regel: `tagged-eks-identityproviderconfig` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon EKS-Identitätsanbieter-Konfiguration Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn die Konfiguration keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Konfiguration mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu Konfigurationen eines EKS-Identitätsanbieters finden Sie unter Taggen Ihrer Amazon EKS-Ressourcen im Amazon EKS-Benutzerhandbuch.

[EKS.8] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (12), NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIst.800-53.R5 AU-10, NIst.800-53.R5 AU-2, NIST.800-53.R5 AU-2 800-53.R5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 AU-9 (7), NIST.800-53.R5 CA-7, NIst.800-53.R5 SC-7 (9), NIst.800-53.R5 SI-3 (8), NIst.800-53.R5 SI-4, NIST.800-53,R5 SI-4 (20), NIST.800-53,R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::EKS::Cluster`

AWS Config -Regel: `eks-cluster-logging-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob für einen Amazon EKS-Cluster die Auditprotokollierung aktiviert ist. Die Kontrolle schlägt fehl, wenn die Audit-Protokollierung für den Cluster nicht aktiviert ist.

Die EKS-Protokollierung auf der Kontrollebene stellt Prüf- und Diagnoseprotokolle direkt von der EKS-Steuerebene zu Amazon CloudWatch Logs in Ihrem Konto bereit. Sie können die Protokolltypen auswählen, die Sie benötigen, und die Protokolle werden als Protokollstreams an eine Gruppe für jeden EKS-Cluster gesendet CloudWatch. Die Protokollierung bietet Einblick in den Zugriff und die Leistung von EKS-Clustern. Indem Sie die Protokolle der EKS-Kontrollebene für Ihre EKS-Cluster an

CloudWatch Logs senden, können Sie Vorgänge zu Prüf- und Diagnosezwecken an einem zentralen Ort aufzeichnen.

Abhilfe

Informationen zum Aktivieren von Audit-Logs für Ihren EKS-Cluster finden Sie unter Aktivieren und Deaktivieren von Control Plane-Protokollen im Amazon EKS-Benutzerhandbuch.

ElastiCache Amazon-Kontrollen

Diese Kontrollen beziehen sich auf ElastiCache Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[ElastiCache.1] Bei ElastiCache Redis-Clustern sollte das automatische Backup aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6, NIST.800-53.R5 CP-6 (1), NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 CP-9, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellen > Resilienz > Backups aktiviert

Schweregrad: Hoch

Ressourcentyp: `AWS::ElastiCache::CacheCluster`

AWS Config Regel: **`elasticache-redis-cluster-automatic-backup-check`**

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`snapshotRetentionPeriod`	Minimale Aufbewahrungsdauer für Snapshots in Tagen	Ganzzahl	1 auf 35	1

Diese Kontrolle bewertet, ob für einen Amazon ElastiCache for Redis-Cluster automatische Backups geplant sind. Die Steuerung schlägt fehl, wenn der `SnapshotRetentionLimit` für den Redis-Cluster angegebene Zeitraum kürzer als der angegebene Zeitraum ist. Sofern Sie keinen benutzerdefinierten Parameterwert für die Aufbewahrungsdauer von Snapshots angeben, verwendet Security Hub einen Standardwert von 1 Tag.

Amazon ElastiCache for Redis-Cluster können ihre Daten sichern. Sie können die Sicherung zur Wiederherstellung eines Clusters oder als Ausgangspunkt für einen neuen Cluster verwenden. Eine Sicherung besteht aus den Metadaten des Clusters zusammen mit allen Daten im Cluster. Alle Sicherungen werden in Amazon Simple Storage Service (Amazon S3) geschrieben, der einen dauerhaften Speicher bereitstellt. Sie können Ihre Daten wiederherstellen, indem Sie einen neuen Redis-Cluster erstellen und ihn mit Daten aus einer Sicherung füllen. Sie können Backups mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) und der ElastiCache API verwalten.

Abhilfe

Informationen zum Planen automatischer Backups auf einem ElastiCache for Redis-Cluster finden Sie unter Automatische Backups planen im ElastiCache Amazon-Benutzerhandbuch.

[ElastiCache.2] ElastiCache Für Redis-Cache-Cluster sollte das auto Upgrade der Nebenversion aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5)

Kategorie: Identifizieren > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::ElastiCache::CacheCluster`

AWS Config -Regel: `elasticache-auto-minor-version-upgrade-check`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement bewertet, ob ElastiCache für Redis automatisch kleinere Versionsupgrades auf Cache-Cluster angewendet werden. Dieses Steuerelement schlägt fehl, wenn ElastiCache für Redis-Cache-Cluster keine Upgrades für Nebenversionen automatisch angewendet werden.

`AutoMinorVersionUpgrade`ist eine Funktion, die Sie ElastiCache für Redis aktivieren können, damit Ihre Cache-Cluster automatisch aktualisiert werden, wenn eine neue kleinere Cache-Engine-Version verfügbar ist. Diese Upgrades können Sicherheitspatches und Bugfixes beinhalten. Die up-to-date Beibehaltung der Patch-Installation ist ein wichtiger Schritt zur Sicherung der Systeme.

Abhilfe

Informationen zum Anwenden automatischer Upgrades kleinerer Versionen auf einen vorhandenen Cache-Cluster ElastiCache für Redis finden Sie unter Upgraden von Engine-Versionen im ElastiCache Amazon-Benutzerhandbuch.

[ElastiCache.3] ElastiCache Für Redis-Replikationsgruppen sollte der automatische Failover aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::ElastiCache::ReplicationGroup`

AWS Config -Regel: `elasticache-repl-grp-auto-failover-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ElastiCache für Redis-Replikationsgruppen das automatische Failover aktiviert ist. Diese Steuerung schlägt fehl, wenn das automatische Failover für eine Redis-Replikationsgruppe nicht aktiviert ist.

Wenn der automatische Failover für eine Replikationsgruppe aktiviert ist, wird für die Rolle des Primärknotens automatisch ein Failover auf eine der Read Replicas ausgeführt. Dieses Failover und die Replikatheraufstufung stellen sicher, dass Sie nach Abschluss der Heraufstufung wieder auf den neuen Primärserver schreiben können, wodurch die Gesamtausfallzeit im Falle eines Fehlers reduziert wird.

Abhilfe

Informationen zum Aktivieren des automatischen Failovers für eine bestehende ElastiCache Redis-Replikationsgruppe finden Sie unter Modifizieren eines ElastiCache Clusters im ElastiCache

Amazon-Benutzerhandbuch. Wenn Sie die ElastiCache Konsole verwenden, setzen Sie Auto Failover auf aktiviert.

[ElastiCache.4] ElastiCache für Redis-Replikationsgruppen sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: `AWS::ElastiCache::ReplicationGroup`

AWS Config -Regel: `elasticache-repl-grp-encrypted-at-rest`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ElastiCache Redis-Replikationsgruppen im Ruhezustand verschlüsselt sind. Dieses Steuerelement schlägt fehl, wenn eine Replikationsgruppe ElastiCache für Redis im Ruhezustand nicht verschlüsselt ist.

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass ein nicht authentifizierter Benutzer Zugriff auf Daten erhält, die auf der Festplatte gespeichert sind. ElastiCache für Redis sollten Replikationsgruppen im Ruhezustand verschlüsselt werden, um eine zusätzliche Sicherheitsebene zu gewährleisten.

Abhilfe

Informationen zur Konfiguration der Verschlüsselung im Ruhezustand ElastiCache für eine Redis-Replikationsgruppe finden Sie unter Enabling at rest encryption im ElastiCache Amazon-Benutzerhandbuch.

[ElastiCache.5] ElastiCache für Redis-Replikationsgruppen sollten bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.R5 AC-17 (2), NIST.800-53.R5 AC-4, NIST.800-53.R5 IA-5 (1), NIst.800-53.R5 SC-12 (3), NIst.800-53.R5 SC-13, NIst.800-53.R5 SC-23, NIst.800-53.R5

SC-23 (3), NIst.NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: `AWS::ElastiCache::ReplicationGroup`

AWS Config -Regel: `elasticache-repl-grp-encrypted-in-transit`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ElastiCache Redis-Replikationsgruppen während der Übertragung verschlüsselt sind. Dieses Steuerelement schlägt fehl, wenn eine Replikationsgruppe ElastiCache für Redis während der Übertragung nicht verschlüsselt wird.

Durch die Verschlüsselung von Daten während der Übertragung wird das Risiko verringert, dass ein nicht autorisierter Benutzer den Netzwerkverkehr abhören kann. Wenn Sie die Verschlüsselung bei der Übertragung in einer Replikationsgruppe ElastiCache für Redis aktivieren, werden Ihre Daten immer dann verschlüsselt, wenn sie von einem Ort an einen anderen übertragen werden, z. B. zwischen Knoten in Ihrem Cluster oder zwischen Ihrem Cluster und Ihrer Anwendung.

Abhilfe

Informationen zur Konfiguration der Verschlüsselung während der Übertragung ElastiCache für eine Redis-Replikationsgruppe finden Sie unter Enabling In-Transit Encryption im ElastiCache Amazon-Benutzerhandbuch.

[ElastiCache.6] ElastiCache Für Redis-Replikationsgruppen vor Version 6.0 sollte Redis AUTH verwendet werden

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-6

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::ElastiCache::ReplicationGroup`

AWS Config -Regel: `elasticache-repl-grp-redis-auth-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Redis AUTH ElastiCache für Redis-Replikationsgruppen aktiviert ist. Das Steuerelement schlägt ElastiCache für eine Redis-Replikationsgruppe fehl, wenn die Redis-Version ihrer Knoten unter 6.0 liegt und `AuthToken` nicht verwendet wird.

Wenn Sie Redis-Authentifizierungstoken oder Passwörter verwenden, benötigt Redis ein Passwort, bevor Clients Befehle ausführen können, was die Datensicherheit verbessert. Für Redis 6.0 und spätere Versionen empfehlen wir die Verwendung von Role-Based Access Control (RBAC). Da RBAC für Redis-Versionen vor 6.0 nicht unterstützt wird, wertet dieses Steuerelement nur Versionen aus, die die RBAC-Funktion nicht verwenden können.

Abhilfe

Informationen zur Verwendung von Redis AUTH ElastiCache für eine Redis-Replikationsgruppe finden Sie unter Ändern des AUTH-Tokens auf einem vorhandenen ElastiCache für Redis Cluster im Amazon-Benutzerhandbuch. ElastiCache

[ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden

Verwandte Anforderungen: NIst.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (5)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::ElastiCache::CacheCluster`

AWS Config -Regel: `elasticache-subnet-group-check`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ElastiCache Cluster mit einer benutzerdefinierten Subnetzgruppe konfiguriert sind. Die Steuerung schlägt für einen ElastiCache Cluster fehl, wenn sie den Wert `CacheSubnetGroupName` `default` hat.

Beim Starten eines ElastiCache Clusters wird eine Standard-Subnetzgruppe erstellt, falls noch keine vorhanden ist. Die Standardgruppe verwendet Subnetze aus der standardmäßigen Virtual Private Cloud (VPC). Wir empfehlen, benutzerdefinierte Subnetzgruppen zu verwenden, die die Subnetze, in denen sich der Cluster befindet, und die Netzwerke, die der Cluster von den Subnetzen erbt, restriktiver behandeln.

Abhilfe

Informationen zum Erstellen einer neuen Subnetzgruppe für einen ElastiCache Cluster finden Sie unter Erstellen einer Subnetzgruppe im ElastiCache Amazon-Benutzerhandbuch.

AWS Elastic Beanstalk steuert

Diese Steuerelemente beziehen sich auf Elastic Beanstalk Beanstalk-Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben

Verwandte Anforderungen: NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-2

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: `AWS::ElasticBeanstalk::Environment`

AWS Config -Regel: `beanstalk-enhanced-health-reporting-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die erweiterte Integritätsberichterstattung für Ihre AWS Elastic Beanstalk Umgebungen aktiviert ist.

Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen.

Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen. Der Elastic Beanstalk Health Agent, der in unterstützten Amazon Machine Images (AMIs) enthalten ist, wertet Logs und Metriken von EC2-Instances in der Umgebung aus.

Weitere Informationen finden Sie unter Verbesserte Statusberichterstattung und Überwachung im Entwicklerhandbuch.AWS Elastic Beanstalk

Abhilfe

Anweisungen zur Aktivierung der erweiterten Zustandsberichterstattung finden Sie unter Enabling enhanced Health Reporting using the Elastic Beanstalk Console im AWS Elastic Beanstalk Developer Guide.

[ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5)

Kategorie: Erkennen > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::ElasticBeanstalk::Environment`

AWS Config -Regel: `elastic-beanstalk-managed-updates-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`UpdateLevel`	Stufe des Versionsupdates	Enum	`minor`, `patch`	Kein Standardwert

Dieses Steuerelement prüft, ob verwaltete Plattformupdates für eine Elastic Beanstalk Beanstalk-Umgebung aktiviert sind. Die Steuerung schlägt fehl, wenn keine Updates für verwaltete Plattformen aktiviert sind. Standardmäßig ist die Steuerung erfolgreich, wenn irgendeine Art von Plattform-Update aktiviert ist. Optional können Sie einen benutzerdefinierten Parameterwert angeben, um eine bestimmte Aktualisierungsstufe zu erfordern.

Durch die Aktivierung verwalteter Plattformupdates wird sichergestellt, dass die neuesten verfügbaren Plattformkorrekturen, Updates und Funktionen für die Umgebung installiert werden. Ein wichtiger Schritt zur Sicherung der Systeme ist es, bei der Patch-Installation auf dem Laufenden zu bleiben.

Abhilfe

Informationen zur Aktivierung verwalteter Plattformupdates finden Sie unter So konfigurieren Sie verwaltete Plattformupdates unter Verwaltete Plattformupdates im AWS Elastic Beanstalk Entwicklerhandbuch.

[ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch

Kategorie: Identifizieren > Protokollierung

Schweregrad: Hoch

Ressourcentyp: `AWS::ElasticBeanstalk::Environment`

AWS Config -Regel: `elastic-beanstalk-logs-to-cloudwatch`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`RetentionInDays`	Anzahl der Tage, an denen Protokollereignisse vor Ablauf aufbewahrt werden sollen	Enum	`1`, `3`, `5`, `7`, `14`, `30`, `60`, `90`, `120`, `150`, `180`, `365` ,	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
			`400`, `545`, `731`, `1827`, `3653`	

Dieses Steuerelement prüft, ob eine Elastic Beanstalk Beanstalk-Umgebung so konfiguriert ist, dass sie Logs an CloudWatch Logs sendet. Die Steuerung schlägt fehl, wenn eine Elastic Beanstalk Beanstalk-Umgebung nicht so konfiguriert ist, dass sie Logs an CloudWatch Logs sendet. Optional können Sie einen benutzerdefinierten Wert für den `RetentionInDays` Parameter angeben, wenn Sie möchten, dass die Steuerung nur dann erfolgreich ist, wenn Logs für die angegebene Anzahl von Tagen vor Ablauf aufbewahrt werden.

CloudWatch hilft Ihnen dabei, verschiedene Messwerte für Ihre Anwendungen und Infrastrukturressourcen zu sammeln und zu überwachen. Sie können es auch verwenden CloudWatch , um Alarmaktionen auf der Grundlage bestimmter Metriken zu konfigurieren. Wir empfehlen die Integration von Elastic Beanstalk mit, CloudWatch um mehr Einblick in Ihre Elastic Beanstalk Beanstalk-Umgebung zu erhalten. Zu den Elastic Beanstalk Beanstalk-Protokollen gehören die Datei eb-activity.log, Zugriffsprotokolle vom Umgebungs-Nginx- oder Apache-Proxyserver sowie umgebungsspezifische Protokolle.

Abhilfe

Informationen zur Integration von Elastic Beanstalk mit CloudWatch Logs finden Sie im AWS Elastic Beanstalk Developer Guide unter CloudWatch Instanzprotokolle streamen.

Elastic Load Balancing Balancing-Steuerelemente

Diese Kontrollen beziehen sich auf Elastic Load Balancing Balancing-Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden

Verwandte Anforderungen: PCI DSS v3.2.1/2.3, PCI DSS v3.2.1/4.1, NIST.800-53.R5 AC-17 (2), NIST.800-53.R5 AC-4, NIST.800-53.R5 IA-5 (1), NIST.800-53.R5 SC-12 (3), NIst.800-53.R5 SC-23, NIST.800-53.R5 SC-23 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: `alb-http-to-https-redirection-check`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die HTTP-zu-HTTPS-Umleitung auf allen HTTP-Listenern von Application Load Balancers konfiguriert ist. Die Steuerung schlägt fehl, wenn für einen der HTTP-Listener von Application Load Balancers keine HTTP-zu-HTTPS-Umleitung konfiguriert ist.

Bevor Sie Ihren Application Load Balancer verwenden können, müssen Sie einen oder mehrere Listener hinzufügen. Ein Listener ist ein Prozess, der das konfigurierte Protokoll und den Port verwendet, um nach Verbindungsanforderungen zu suchen. Listener unterstützen sowohl das HTTP- als auch das HTTPS-Protokoll. Sie können einen HTTPS-Listener verwenden, um die Arbeit der Verschlüsselung und Entschlüsselung auf Ihren Load Balancer auszulagern. Um die Verschlüsselung während der Übertragung zu erzwingen, sollten Sie Umleitungsaktionen mit Application Load Balancers verwenden, um Client-HTTP-Anfragen an eine HTTPS-Anfrage an Port 443 umzuleiten.

Weitere Informationen finden Sie unter Listener für Ihre Application Load Balancers im Benutzerhandbuch für Application Load Balancers.

Abhilfe

Um HTTP-Anfragen an HTTPS umzuleiten, müssen Sie eine Application Load Balancer Balancer-Listener-Regel hinzufügen oder eine bestehende Regel bearbeiten.

Anweisungen zum Hinzufügen einer neuen Regel finden Sie unter Regel hinzufügen im Benutzerhandbuch für Application Load Balancers. Wählen Sie für Protocol: Port die Option HTTP

und geben Sie dann ein**80**. Wählen Sie für Aktion hinzufügen die Option Umleiten zu die Option HTTPS aus, und geben Sie dann die Eingabetaste ein**443**.

Anweisungen zum Bearbeiten einer vorhandenen Regel finden Sie unter Regel bearbeiten im Benutzerhandbuch für Application Load Balancers. Wählen Sie für Protocol: Port die Option HTTP und geben Sie dann ein**80**. Wählen Sie für Aktion hinzufügen die Option Umleiten zu die Option HTTPS aus, und geben Sie dann die Eingabetaste ein**443**.

[ELB.2] Classic Load Balancer mit SSL/HTTPS-Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager

Verwandte Anforderungen: NIst.800-53.R5 AC-17 (2), NIST.800-53.R5 AC-4, NIST.800-53.R5 IA-5 (1), NIst.800-53.R5 SC-12 (3), NIST.800-53.R5 SC-13, NIst.800-53.R5 SC-23, NIst.800-53.R5 SC-23 (5), NIst.NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategorie: Schützen > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config -Regel: `elb-acm-certificate-required`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Classic Load Balancer HTTPS/SSL-Zertifikate verwendet, die von AWS Certificate Manager (ACM) bereitgestellt werden. Die Steuerung schlägt fehl, wenn der mit dem HTTPS/SSL-Listener konfigurierte Classic Load Balancer kein von ACM bereitgestelltes Zertifikat verwendet.

Um ein Zertifikat zu erstellen, können Sie entweder ACM oder ein Tool verwenden, das die SSL- und TLS-Protokolle unterstützt, z. B. OpenSSL. Security Hub empfiehlt, dass Sie ACM verwenden, um Zertifikate für Ihren Load Balancer zu erstellen oder zu importieren.

ACM ist in Classic Load Balancers integriert, sodass Sie das Zertifikat auf Ihrem Load Balancer bereitstellen können. Sie sollten diese Zertifikate auch automatisch erneuern.

Abhilfe

Informationen zum Zuordnen eines ACM-SSL/TLS-Zertifikats zu einem Classic Load Balancer finden Sie im AWS Knowledge Center-Artikel Wie kann ich ein ACM-SSL/TLS-Zertifikat mit einem Classic-, Anwendungs- oder Network Load Balancer verknüpfen?

[ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden

Verwandte Anforderungen: NIST.800-53.R5 AC-17 (2), NIST.800-53.R5 AC-4, NIST.800-53.R5 IA-5 (1), NIst.800-53.R5 SC-12 (3), NIst.800-53.R5 SC-13, NIst.800-53.R5 SC-23, NIst.800-53.R5 SC-23 (3), NIst.NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten währen der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config -Regel: `elb-tls-https-listeners-only`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Ihre Classic Load Balancer Balancer-Listener mit dem HTTPS- oder TLS-Protokoll für Front-End-Verbindungen (Client zu Load Balancer) konfiguriert sind. Die Steuerung ist anwendbar, wenn ein Classic Load Balancer über Listener verfügt. Wenn für Ihren Classic Load Balancer kein Listener konfiguriert ist, meldet die Steuerung keine Ergebnisse.

Die Steuerung ist erfolgreich, wenn die Classic Load Balancer Balancer-Listener mit TLS oder HTTPS für Frontend-Verbindungen konfiguriert sind.

Die Steuerung schlägt fehl, wenn der Listener nicht mit TLS oder HTTPS für Frontend-Verbindungen konfiguriert ist.

Bevor Sie mit der Verwendung eines Load Balancers beginnen, müssen Sie einen oder mehrere Listener hinzufügen. Ein Listener ist ein Prozess, der das konfigurierte Protokoll und den Port verwendet, um nach Verbindungsanforderungen zu suchen. Listener können sowohl HTTP- als auch

HTTPS/TLS-Protokolle unterstützen. Sie sollten immer einen HTTPS- oder TLS-Listener verwenden, damit der Load Balancer die Ver- und Entschlüsselung während der Übertragung übernimmt.

Abhilfe

Um dieses Problem zu beheben, aktualisieren Sie Ihre Listener so, dass sie das TLS- oder HTTPS-Protokoll verwenden.

Um alle nicht konformen Listener in TLS/HTTPS-Listener umzuwandeln

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Load Balancing die Option Load Balancers aus.
3. Wählen Sie Ihren Classic Load Balancer aus.
4. Wählen Sie auf der Registerkarte Listeners die Option Edit aus.
5. Ändern Sie für alle Listener, bei denen das Load Balancer-Protokoll nicht auf HTTPS oder SSL eingestellt ist, die Einstellung auf HTTPS oder SSL.
6. Wählen Sie für alle modifizierten Listener auf der Registerkarte Zertifikate die Option Standard ändern aus.
7. Wählen Sie für ACM- und IAM-Zertifikate ein Zertifikat aus.
8. Wählen Sie Als Standard speichern aus.
9. Nachdem Sie alle Listener aktualisiert haben, wählen Sie Speichern.

[ELB.4] Application Load Balancer sollte so konfiguriert sein, dass HTTP-Header gelöscht werden

Verwandte Anforderungen: NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8 (2)

Kategorie: Schützen > Netzwerksicherheit

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: `alb-http-drop-invalid-header-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement bewertet AWS Application Load Balancer, um sicherzustellen, dass sie so konfiguriert sind, dass sie ungültige HTTP-Header löschen. Das Steuerelement schlägt fehl, wenn der Wert von auf gesetzt `routing.http.drop_invalid_header_fields.enabled` ist. `false`

Standardmäßig sind Application Load Balancer nicht so konfiguriert, dass sie ungültige HTTP-Header-Werte löschen. Durch das Entfernen dieser Header-Werte werden HTTP-Desync-Angriffe verhindert.

Beachten Sie, dass Sie dieses Steuerelement deaktivieren können, wenn ELB.12 aktiviert ist.

Abhilfe

Um dieses Problem zu beheben, konfigurieren Sie Ihren Load Balancer so, dass ungültige Header-Felder gelöscht werden.

Um den Load Balancer so zu konfigurieren, dass ungültige Header-Felder gelöscht werden

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Load balancers (Load Balancer).
3. Wählen Sie einen Application Load Balancer aus.
4. Wählen Sie unter Aktionen die Option Attribute bearbeiten aus.
5. Wählen Sie unter Ungültige Header-Felder löschen die Option Aktivieren aus.
6. Wählen Sie Speichern.

[ELB.5] Die Protokollierung von Anwendungen und Classic Load Balancers sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-3. R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Ressourcentyp:`AWS::ElasticLoadBalancing::LoadBalancer`, `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: `elb-logging-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Application Load Balancer und der Classic Load Balancer die Protokollierung aktiviert haben. Ist dies der Fall, schlägt die Steuerung fehl. `access_logs.s3.enabled` `false`

Elastic Load Balancing bietet Zugriffsprotokolle, die detaillierte Informationen zu Anforderungen erfassen, die an Ihren Load Balancer gesendet werden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten. Sie können diese Zugriffsprotokolle für die Analyse von Datenverkehrsmustern und zur Problembehebung verwenden.

Weitere Informationen finden Sie unter Zugriffsprotokolle für Ihren Classic Load Balancer im Benutzerhandbuch für Classic Load Balancer.

Abhilfe

Informationen zum Aktivieren von Zugriffsprotokollen finden Sie unter Schritt 3: Zugriffsprotokolle konfigurieren im Benutzerhandbuch für Application Load Balancers.

[ELB.6] Für Anwendungen, Gateways und Network Load Balancers sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2), NIST.800-53.R5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: `elb-deletion-protection-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Anwendung, ein Gateway oder ein Network Load Balancer der Löschschutz aktiviert ist. Die Steuerung schlägt fehl, wenn der Löschschutz deaktiviert ist.

Aktivieren Sie den Löschschutz, um Ihre Anwendung, Ihr Gateway oder Ihren Network Load Balancer vor dem Löschen zu schützen.

Abhilfe

Um zu verhindern, dass der Load Balancer versehentlich gelöscht wird, können Sie den Löschschutz aktivieren. Standardmäßig ist der Löschschutz für Ihren Load Balancer deaktiviert.

Wenn Sie den Löschschutz für Ihren Load Balancer aktivieren, müssen Sie den Löschschutz deaktivieren, bevor Sie den Load Balancer löschen können.

Informationen zum Aktivieren des Löschschutzes für einen Application Load Balancer finden Sie unter Löschschutz im Benutzerhandbuch für Application Load Balancer. Informationen zum Aktivieren des Löschschutzes für einen Gateway Load Balancer finden Sie unter Löschschutz im Benutzerhandbuch für Gateway Load Balancer. Informationen zum Aktivieren des Löschschutzes für einen Network Load Balancer finden Sie unter Löschschutz im Benutzerhandbuch für Network Load Balancer.

[ELB.7] Bei Classic Load Balancers sollte der Verbindungsverlust aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Erholung > Resilienz

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config Regel: `elb-connection-draining-enabled` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob bei Classic Load Balancers der Verbindungsabbau aktiviert ist.

Durch die Aktivierung des Verbindungsabbaus auf Classic Load Balancers wird sichergestellt, dass der Load Balancer keine Anfragen mehr an Instances sendet, die sich abmelden oder deren Status beeinträchtigt ist. Es hält die bestehenden Verbindungen offen. Dies ist besonders nützlich

für Instances in Auto Scaling Scaling-Gruppen, um sicherzustellen, dass Verbindungen nicht abrupt unterbrochen werden.

Abhilfe

Informationen zum Aktivieren des Verbindungsabbaus auf Classic Load Balancers finden Sie unter Connection Draining für Ihren Classic Load Balancer konfigurieren im Benutzerhandbuch für Classic Load Balancers.

[ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config

Verwandte Anforderungen: NIST.800-53.R5 AC-17 (2), NIST.800-53.R5 AC-4, NIST.800-53.R5 IA-5 (1), NIst.800-53.R5 SC-12 (3), NIst.800-53.R5 SC-13, NIst.800-53.R5 SC-23, NIst.800-53.R5 SC-23 (3), NIst.NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategorie: Schützen > Verschlüsselung von Daten bei der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config -Regel: `elb-predefined-security-policy-ssl-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `predefinedPolicyName`: `ELBSecurityPolicy-TLS-1-2-2017-01` (nicht anpassbar)

Dieses Steuerelement prüft, ob Ihre Classic Load Balancer HTTPS/SSL-Listener die vordefinierte Richtlinie verwenden. `ELBSecurityPolicy-TLS-1-2-2017-01` Die Steuerung schlägt fehl, wenn die Classic Load Balancer HTTPS/SSL-Listener sie nicht verwenden. `ELBSecurityPolicy-TLS-1-2-2017-01`

Eine Sicherheitsrichtlinie ist eine Kombination aus SSL-Protokollen, Chiffren und der Option Server Order Preference. Vordefinierte Richtlinien steuern die Chiffren, Protokolle und Präferenzreihenfolgen, die bei SSL-Verhandlungen zwischen einem Client und einem Load Balancer unterstützt werden sollen.

Die Verwendung `ELBSecurityPolicy-TLS-1-2-2017-01` kann Ihnen dabei helfen, die Compliance- und Sicherheitsstandards zu erfüllen, nach denen Sie bestimmte Versionen von SSL und TLS deaktivieren müssen. Weitere Informationen finden Sie unter Vordefinierte SSL-Sicherheitsrichtlinien für Classic Load Balancers im Benutzerhandbuch für Classic Load Balancers.

Abhilfe

Informationen zur Verwendung der vordefinierten Sicherheitsrichtlinie `ELBSecurityPolicy-TLS-1-2-2017-01` mit einem Classic Load Balancer finden Sie unter Sicherheitseinstellungen konfigurieren im Benutzerhandbuch für Classic Load Balancers.

[ELB.9] Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config -Regel: `elb-cross-zone-load-balancing-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der zonenübergreifende Load Balancing für die Classic Load Balancers (CLBs) aktiviert ist. Die Steuerung schlägt fehl, wenn der zonenübergreifende Lastenausgleich für einen CLB nicht aktiviert ist.

Ein Load Balancer-Knoten verteilt den Verkehr nur auf die registrierten Ziele in seiner Availability Zone. Wenn zonenübergreifendes Load Balancing deaktiviert ist, verteilt jeder Load Balancer-Knoten den Datenverkehr gleichmäßig nur auf die registrierten Ziele in seiner Availability Zone. Wenn die Anzahl der registrierten Ziele in den Availability Zones nicht identisch ist, wird der Verkehr nicht gleichmäßig verteilt und die Instances in einer Zone werden möglicherweise im Vergleich zu den Instances in einer anderen Zone überlastet. Wenn zonenübergreifendes Load Balancing aktiviert ist, verteilt jeder Load Balancer-Knoten für Ihren Classic Load Balancer Anfragen gleichmäßig

auf die registrierten Instances in allen aktivierten Availability Zones. Einzelheiten finden Sie unter Zonenübergreifendes Load Balancing im Elastic Load Balancing User Guide.

Abhilfe

Informationen zur Aktivierung von zonenübergreifendem Load Balancing in einem Classic Load Balancer finden Sie unter Aktivieren von zonenübergreifendem Load Balancing im Benutzerhandbuch für Classic Load Balancer.

[ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIst.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config -Regel: `clb-multiple-az`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`minAvailabilityZones`	Mindestanzahl von Availability Zones	Enum	`2, 3, 4, 5, 6`	`2`

Dieses Steuerelement prüft, ob ein Classic Load Balancer so konfiguriert wurde, dass er sich über mindestens die angegebene Anzahl von Availability Zones (AZs) erstreckt. Die Steuerung schlägt fehl, wenn der Classic Load Balancer nicht mindestens die angegebene Anzahl von AZs umfasst. Sofern Sie keinen benutzerdefinierten Parameterwert für die Mindestanzahl von AZs angeben, verwendet Security Hub einen Standardwert von zwei AZs.

Ein Classic Load Balancer kann so eingerichtet werden, dass eingehende Anfragen auf Amazon EC2 EC2-Instances in einer einzigen Availability Zone oder mehreren Availability Zones verteilt werden. Ein Classic Load Balancer, der sich nicht über mehrere Availability Zones erstreckt, kann den Traffic nicht zu Zielen in einer anderen Availability Zone umleiten, wenn die einzige konfigurierte Availability Zone nicht mehr verfügbar ist.

Abhilfe

Informationen zum Hinzufügen von Availability Zones zu einem Classic Load Balancer finden Sie unter Hinzufügen oder Entfernen von Subnetzen für Ihren Classic Load Balancer im Benutzerhandbuch für Classic Load Balancer.

[ELB.12] Application Load Balancer sollte mit dem defensiven Modus oder dem strengsten Modus zur Desynchronisierung konfiguriert werden

Verwandte Anforderungen: NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Datenschutz > Datenintegrität

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: `alb-desync-mode-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `desyncMode`: `defensive, strictest` (nicht anpassbar)

Dieses Steuerelement prüft, ob ein Application Load Balancer mit dem defensiven Modus oder dem strengsten Modus zur Desynchronisierung konfiguriert ist. Die Steuerung schlägt fehl, wenn ein Application Load Balancer nicht mit dem defensiven Modus oder dem strengsten Modus zur Desynchronisierung konfiguriert ist.

Probleme mit der HTTP-Desynchronisierung können zum Schmuggel von Anfragen führen und Anwendungen anfällig für Queue-Anfragen oder Cache-Poisoning machen. Diese Sicherheitsanfälligkeiten können wiederum dazu führen, dass Anmeldeinformationen überlastet

werden oder nicht autorisierte Befehle ausgeführt werden. Application Load Balancer, die mit dem defensiven Modus oder der striktesten Abschwächung der Desynchronisierung konfiguriert sind, schützen Ihre Anwendung vor Sicherheitsproblemen, die durch HTTP-Desync verursacht werden können.

Abhilfe

Informationen zum Aktualisieren des Desync-Minimationsmodus eines Application Load Balancer finden Sie unter Desync-Minimationsmodus im Benutzerhandbuch für Application Load Balancers.

[ELB.13] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: `elbv2-multiple-az`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`minAvailabilityZones`	Mindestanzahl von Availability Zones	Enum	`2, 3, 4, 5, 6`	2

Dieses Steuerelement prüft, ob ein Elastic Load Balancer V2 (Application, Network oder Gateway Load Balancer) Instances aus mindestens der angegebenen Anzahl von Availability Zones (AZs)

registriert hat. Die Kontrolle schlägt fehl, wenn bei einem Elastic Load Balancer V2 keine Instances in mindestens der angegebenen Anzahl von AZs registriert sind. Sofern Sie keinen benutzerdefinierten Parameterwert für die Mindestanzahl von AZs angeben, verwendet Security Hub einen Standardwert von zwei AZs.

Elastic Load Balancing verteilt Ihren eingehenden Datenverkehr automatisch auf mehrere Ziele, z. B. EC2-Instances, Container und IP-Adressen oder eine oder mehrere Availability Zones. Elastic Load Balancing skaliert Ihren Load Balancer, wenn sich der eingehende Datenverkehr im Laufe der Zeit ändert. Es wird empfohlen, mindestens zwei Availability Zones zu konfigurieren, um die Verfügbarkeit von Diensten sicherzustellen, da der Elastic Load Balancer den Traffic in eine andere Availability Zone weiterleiten kann, falls eine nicht verfügbar ist. Die Konfiguration mehrerer Availability Zones trägt dazu bei, dass es keine einzige Fehlerquelle für die Anwendung gibt.

Abhilfe

Informationen zum Hinzufügen einer Availability Zone zu einem Application Load Balancer finden Sie unter Availability Zones for your Application Load Balancer im Benutzerhandbuch für Application Load Balancer. Informationen zum Hinzufügen einer Availability Zone zu einem Network Load Balancer finden Sie unter Network Load Balancers im Benutzerhandbuch für Network Load Balancer. Informationen zum Hinzufügen einer Availability Zone zu einem Gateway Load Balancer finden Sie unter Erstellen eines Gateway Load Balancers im Benutzerhandbuch für Gateway Load Balancer.

[ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden

Verwandte Anforderungen: NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Datenschutz > Datenintegrität

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config -Regel: `clb-desync-mode-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `desyncMode`: `defensive, strictest` (nicht anpassbar)

Dieses Steuerelement prüft, ob ein Classic Load Balancer mit einem defensiven oder dem strengsten Desync-Minimierungsmodus konfiguriert ist. Die Steuerung schlägt fehl, wenn der Classic Load Balancer nicht mit dem defensiven Modus oder dem strengsten Modus zur Desynchronisierung konfiguriert ist.

Probleme mit der HTTP-Desynchronisierung können zum Schmuggel von Anfragen führen und Anwendungen anfällig für Queue-Anfragen oder Cache-Poisoning machen. Diese Sicherheitsanfälligkeiten können wiederum zur Entführung von Anmeldeinformationen oder zur Ausführung nicht autorisierter Befehle führen. Classic Load Balancer, die mit dem defensiven Modus oder der striktesten Abschwächung der Desynchronisierung konfiguriert sind, schützen Ihre Anwendung vor Sicherheitsproblemen, die durch HTTP-Desync verursacht werden können.

Abhilfe

Informationen zum Aktualisieren des Desync-Mitigationsmodus auf einem Classic Load Balancer finden Sie unter Ändern des Desync-Mitigationsmodus im Benutzerhandbuch für Classic Load Balancer.

[ELB.16] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF

Verwandte Anforderungen: NIST.800-53.r5 AC-4 (21)

Kategorie: Schützen > Schutzdienste

Schweregrad: Mittel

Art der Ressource: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config -Regel: `alb-waf-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Application Load Balancer einer AWS WAF Classic- oder AWS WAF Web-Zugriffskontrollliste (Web-ACL) zugeordnet ist. Die Steuerung schlägt fehl, wenn das `Enabled` Feld für die AWS WAF Konfiguration auf `false` gesetzt ist.

AWS WAF ist eine Firewall für Webanwendungen, die hilft, Webanwendungen und APIs vor Angriffen zu schützen. Mit AWS WAF können Sie eine Web-ACL konfigurieren, bei der es sich um eine Reihe von Regeln handelt, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Wir empfehlen, Ihren Application Load Balancer mit einer AWS WAF Web-ACL zu verknüpfen, um ihn vor böswilligen Angriffen zu schützen.

Abhilfe

Informationen zum Zuordnen eines Application Load Balancer zu einer Web-ACL finden Sie unter Web-ACL mit einer AWS Ressource verknüpfen oder deren Zuordnung aufheben im Developer Guide.AWS WAF

Amazon EMR-Steuerelemente

Diese Kontrollen beziehen sich auf Amazon EMR-Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.R5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.R5 AC-3. R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21)), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::EMR::Cluster`

AWS Config -Regel: `emr-master-no-public-ip`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Master-Knoten auf Amazon EMR-Clustern öffentliche IP-Adressen haben. Die Kontrolle schlägt fehl, wenn öffentliche IP-Adressen einer der Master-Node-Instances zugeordnet sind.

Öffentliche IP-Adressen werden im `PublicIp` Feld der `NetworkInterfaces` Konfiguration für die Instanz angegeben. Dieses Steuerelement überprüft nur Amazon EMR-Cluster, die sich im `WAITING` Status `RUNNING` oder befinden.

Abhilfe

Während des Starts können Sie steuern, ob Ihrer Instance in einem Standard- oder einem anderen Subnetz eine öffentliche IPv4-Adresse zugewiesen wird. In Standard-Subnetzen ist dieses Attribut standardmäßig auf gesetzt. `true` Bei nicht standardmäßigen Subnetzen ist das IPv4-Attribut für öffentliche Adressierung auf gesetzt`false`, sofern es nicht vom Amazon EC2 EC2-Instance-Startassistenten erstellt wurde. In diesem Fall ist das Attribut auf gesetzt. `true`

Nach dem Start können Sie eine öffentliche IPv4-Adresse nicht manuell von Ihrer Instance trennen.

Um ein fehlgeschlagenes Ergebnis zu beheben, müssen Sie einen neuen Cluster in einer VPC mit einem privaten Subnetz starten, für das das IPv4-Attribut für öffentliche Adressierung auf gesetzt ist. `false` Anweisungen finden Sie unter Cluster in einer VPC starten im Amazon EMR Management Guide.

[EMR.2] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schützen > Sicheres Zugriffsmanagement > Ressource nicht öffentlich zugänglich

Schweregrad: Kritisch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `emr-block-public-access`

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob Ihr Konto mit Amazon EMR konfiguriert ist, um den öffentlichen Zugriff zu blockieren. Die Kontrolle schlägt fehl, wenn die Einstellung „Öffentlichen Zugriff blockieren“ nicht aktiviert ist oder wenn ein anderer Port als Port 22 zulässig ist.

Amazon EMR Block Public Access verhindert, dass Sie einen Cluster in einem öffentlichen Subnetz starten, wenn der Cluster über eine Sicherheitskonfiguration verfügt, die eingehenden Datenverkehr von öffentlichen IP-Adressen an einem Port zulässt. Wenn ein Benutzer von Ihrem AWS-Konto einen Cluster startet, überprüft Amazon EMR die Portregeln in der Sicherheitsgruppe für den Cluster und vergleicht sie mit Ihren Regeln für eingehenden Datenverkehr. Wenn die Sicherheitsgruppe über eine Regel für eingehenden Datenverkehr verfügt, die Ports zu den öffentlichen IP-Adressen IPv4 0.0.0.0/0 oder IPv6: :/0 öffnet, und diese Ports nicht als Ausnahmen für Ihr Konto angegeben sind, lässt Amazon EMR den Benutzer den Cluster nicht erstellen.

> **Note**
>
> Den öffentlichen Zugriff blockieren ist standardmäßig aktiviert. Um den Kontoschutz zu erhöhen, empfehlen wir, ihn aktiviert zu lassen.

Abhilfe

Informationen zur Konfiguration von Block Public Access für Amazon EMR finden Sie unter Using Amazon EMR block public access im Amazon EMR Management Guide.

Elasticsearch-Steuerelemente

Diese Kontrollen beziehen sich auf Elasticsearch-Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[ES.1] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein

Verwandte Anforderungen: PCI DSS v3.2.1/3.4, NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIst.800-53.R5 SC-7 (10), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 -53,5R-5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config -Regel: `elasticsearch-encrypted-at-rest`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob für Elasticsearch-Domains die Konfiguration „Verschlüsselung im Ruhezustand“ aktiviert ist. Die Prüfung schlägt fehl, wenn die Verschlüsselung im Ruhezustand nicht aktiviert ist.

Für eine zusätzliche Sicherheitsebene für Ihre sensiblen Daten sollten Sie Ihre Daten so konfigurieren OpenSearch, OpenSearch dass sie im Ruhezustand verschlüsselt werden. Elasticsearch-Domains bieten die Verschlüsselung von Daten im Ruhezustand. Die Funktion dient AWS KMS zum Speichern und Verwalten Ihrer Verschlüsselungsschlüssel. Um die Verschlüsselung durchzuführen, verwendet es den Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256).

Weitere Informationen zur OpenSearch Verschlüsselung im Ruhezustand finden Sie unter Verschlüsselung ruhender Daten für Amazon OpenSearch Service im Amazon OpenSearch Service Developer Guide.

Bestimmte Instance-Typen, wie z. B. `t.small` und`t.medium`, unterstützen die Verschlüsselung von Daten im Ruhezustand nicht. Einzelheiten finden Sie unter Unterstützte Instance-Typen im Amazon OpenSearch Service Developer Guide.

Abhilfe

Informationen zur Aktivierung der Verschlüsselung im Ruhezustand für neue und bestehende Elasticsearch-Domains finden Sie unter Enabling encryption of data at rest im Amazon OpenSearch Service Developer Guide.

[ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.R5 AC-21, NIST.800-53.r5 AC-3,

NIST.800-53.r5 AC-3 (7), NIST.800-53.R5 AC-3. R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21)), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Kritisch

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config -Regel: `elasticsearch-in-vpc-only`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob sich Elasticsearch-Domains in einer VPC befinden. Es bewertet nicht die Konfiguration des VPC-Subnetz-Routings, um den öffentlichen Zugriff zu bestimmen. Sie sollten sicherstellen, dass Elasticsearch-Domains nicht an öffentliche Subnetze angehängt sind. Informationen zu ressourcenbasierten Richtlinien finden Sie im Amazon OpenSearch Service Developer Guide. Sie sollten auch sicherstellen, dass Ihre VPC gemäß den empfohlenen bewährten Methoden konfiguriert ist. Bewährte Sicherheitsmethoden für Ihre VPC finden Sie im Amazon VPC-Benutzerhandbuch.

Elasticsearch-Domains, die in einer VPC bereitgestellt werden, können über das private AWS Netzwerk mit VPC-Ressourcen kommunizieren, ohne das öffentliche Internet durchqueren zu müssen. Diese Konfiguration erhöht die Sicherheitslage, indem der Zugriff auf die Daten während der Übertragung eingeschränkt wird. VPCs bieten eine Reihe von Netzwerksteuerungen, um den Zugriff auf Elasticsearch-Domänen zu sichern, darunter Netzwerk-ACL und Sicherheitsgruppen. Security Hub empfiehlt, öffentliche Elasticsearch-Domains zu VPCs zu migrieren, um diese Kontrollen nutzen zu können.

Abhilfe

Wenn Sie eine Domäne mit einem öffentlichen Endpunkt erstellen, können Sie sie später nicht in einer VPC platzieren. Sie müssen stattdessen eine neue Domäne erstellen und die Daten übernehmen. Umgekehrt gilt dies auch. Wenn Sie eine Domäne innerhalb einer VPC erstellen, kann sie keinen öffentlichen Endpunkt haben. Stattdessen müssen Sie entweder eine andere Domäne erstellen oder dieses Steuerelement deaktivieren.

Weitere Informationen finden Sie unter Starten Ihrer Amazon OpenSearch Service-Domains innerhalb einer VPC im Amazon OpenSearch Service Developer Guide.

[ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

Verwandte Anforderungen: NIst.800-53.R5 AC-4, NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-23, NIST.800-53.R5 SC-23 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIst.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 R5 SC-8 (2)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten währen der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config -Regel: `elasticsearch-node-to-node-encryption-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine Elasticsearch-Domain die node-to-node Verschlüsselung aktiviert ist. Die Steuerung schlägt fehl, wenn für die Elasticsearch-Domain keine node-to-node Verschlüsselung aktiviert ist. Die Kontrolle führt auch zu fehlgeschlagenen Ergebnissen, wenn eine Elasticsearch-Version keine node-to-node Verschlüsselungsprüfungen unterstützt.

HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer den Netzwerkverkehr mit oder ähnlichen Angriffen abhören oder manipulieren. person-in-the-middle Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Durch die Aktivierung der node-to-node Verschlüsselung für Elasticsearch-Domains wird sichergestellt, dass die Kommunikation innerhalb des Clusters während der Übertragung verschlüsselt wird.

Mit dieser Konfiguration kann es zu Leistungseinbußen kommen. Sie sollten sich der Leistungseinbußen bewusst sein und diese testen, bevor Sie diese Option aktivieren.

Abhilfe

Informationen zur Aktivierung der node-to-node Verschlüsselung für neue und bestehende Domains finden Sie unter node-to-nodeEnabling encryption im Amazon OpenSearch Service Developer Guide.

[ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.r5 AU-3 R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren - Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config -Regel: `elasticsearch-logs-to-cloudwatch`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `logtype = 'error'`(nicht anpassbar)

Dieses Steuerelement prüft, ob Elasticsearch-Domains so konfiguriert sind, dass sie CloudWatch Fehlerprotokolle an Logs senden.

Sie sollten Fehlerprotokolle für Elasticsearch-Domains aktivieren und diese CloudWatch Protokolle zur Aufbewahrung und Beantwortung an Logs senden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Abhilfe

Informationen zur Aktivierung der Protokollveröffentlichung finden Sie unter Aktivieren der Protokollveröffentlichung (Konsole) im Amazon OpenSearch Service Developer Guide.

[ES.5] Für Elasticsearch-Domains sollte die Audit-Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.r5 AU-3 R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config Regel: `elasticsearch-audit-logging-enabled` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

- `cloudWatchLogsLogGroupArnList`(nicht anpassbar). Security Hub füllt diesen Parameter nicht aus. Durch Kommas getrennte Liste von CloudWatch Logs-Log-Gruppen, die für Audit-Logs konfiguriert werden sollten.

  Diese Regel gilt, `NON_COMPLIANT` wenn die CloudWatch Logs-Log-Gruppe der Elasticsearch-Domain in dieser Parameterliste nicht angegeben ist.

Dieses Steuerelement prüft, ob für Elasticsearch-Domains die Audit-Protokollierung aktiviert ist. Diese Kontrolle schlägt fehl, wenn für eine Elasticsearch-Domain die Audit-Protokollierung nicht aktiviert ist.

Audit-Logs sind hochgradig anpassbar. Sie ermöglichen es Ihnen, Benutzeraktivitäten auf Ihren Elasticsearch-Clustern nachzuverfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Abhilfe

Ausführliche Anweisungen zur Aktivierung von Audit-Logs finden Sie unter Aktivieren von Audit-Logs im Amazon OpenSearch Service Developer Guide.

[ES.6] Elasticsearch-Domains sollten mindestens drei Datenknoten haben

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config Regel: `elasticsearch-data-node-fault-tolerance` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Elasticsearch-Domänen mit mindestens drei Datenknoten konfiguriert sind und `zoneAwarenessEnabled` ist`true`.

Eine Elasticsearch-Domain benötigt aus Gründen der Hochverfügbarkeit und Fehlertoleranz mindestens drei Datenknoten. Die Bereitstellung einer Elasticsearch-Domain mit mindestens drei Datenknoten gewährleistet den Clusterbetrieb, falls ein Knoten ausfällt.

Abhilfe

Um die Anzahl der Datenknoten in einer Elasticsearch-Domain zu ändern

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/.
2. Wählen Sie unter Domains den Namen der Domain aus, die Sie bearbeiten möchten.
3. Wählen Sie Edit domain (Domäne bearbeiten).
4. Stellen Sie unter Datenknoten die Anzahl der Knoten auf eine Zahl ein, die größer oder gleich ist`3`.

   Legen Sie für Bereitstellungen mit drei Availability Zones den Wert auf ein Vielfaches von drei fest, um eine gleichmäßige Verteilung auf die Availability Zones sicherzustellen.
5. Wählen Sie Absenden aus.

[ES.7] Elasticsearch-Domänen sollten mit mindestens drei dedizierten Master-Knoten konfiguriert werden

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config Regel: `elasticsearch-primary-node-fault-tolerance` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Elasticsearch-Domänen mit mindestens drei dedizierten Primärknoten konfiguriert sind. Diese Kontrolle schlägt fehl, wenn die Domain keine dedizierten Primärknoten verwendet. Diese Kontrolle gilt als bestanden, wenn Elasticsearch-Domänen über fünf dedizierte Primärknoten verfügen. Die Verwendung von mehr als drei Primärknoten ist jedoch möglicherweise unnötig, um das Verfügbarkeitsrisiko zu minimieren, und führt zu zusätzlichen Kosten.

Für eine Elasticsearch-Domain sind mindestens drei dedizierte Primärknoten erforderlich, um eine hohe Verfügbarkeit und Fehlertoleranz zu gewährleisten. Dedizierte Primärknotenressourcen können bei Bereitstellungen mit blauen/grünen Datenknoten belastet werden, da zusätzliche Knoten verwaltet werden müssen. Die Bereitstellung einer Elasticsearch-Domain mit mindestens drei dedizierten Primärknoten gewährleistet eine ausreichende Ressourcenkapazität des Primärknotens und den Clusterbetrieb, falls ein Knoten ausfällt.

Abhilfe

Um die Anzahl der dedizierten Primärknoten in einer OpenSearch Domain zu ändern

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/.
2. Wählen Sie unter Domains den Namen der Domain aus, die Sie bearbeiten möchten.
3. Wählen Sie Edit domain (Domäne bearbeiten).
4. Stellen Sie unter Dedizierte Masterknoten den Instanztyp auf den gewünschten Instanztyp ein.
5. Stellen Sie die Anzahl der Master-Knoten auf drei oder mehr ein.
6. Wählen Sie Absenden aus.

[ES.8] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.R5 AC-17 (2), NIST.800-53.R5 AC-4, NIST.800-53.R5 IA-5 (1), NIst.800-53.R5 SC-12 (3), NIst.800-53.R5 SC-13, NIst.800-53.R5 SC-23, NIst.800-53.R5

SC-23 (3), NIst.NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten währen der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config Regel: `elasticsearch-https-required` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dadurch wird geprüft, ob ein Elasticsearch-Domain-Endpunkt so konfiguriert ist, dass er die neueste TLS-Sicherheitsrichtlinie verwendet. Die Steuerung schlägt fehl, wenn der Elasticsearch-Domänenendpunkt nicht für die Verwendung der neuesten unterstützten Richtlinie konfiguriert ist oder wenn HTTPS nicht aktiviert ist. Die aktuell neueste unterstützte TLS-Sicherheitsrichtlinie ist`Policy-Min-TLS-1-2-PFS-2023-10`.

HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer person-in-the-middle oder ähnliche Angriffe verwenden, um den Netzwerkverkehr zu belauschen oder zu manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Die Verschlüsselung von Daten während der Übertragung kann die Leistung beeinträchtigen. Sie sollten Ihre Anwendung mit dieser Funktion testen, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen. TLS 1.2 bietet mehrere Sicherheitsverbesserungen gegenüber früheren Versionen von TLS.

Abhilfe

Um die TLS-Verschlüsselung zu aktivieren, verwenden Sie den UpdateDomainConfigAPI-Vorgang, um das DomainEndpointOptionsObjekt zu konfigurieren. Dies legt die fest`TLSSecurityPolicy`.

[ES.9] Elasticsearch-Domains sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Elasticsearch::Domain`

AWS Config Regel: `tagged-elasticsearch-domain` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob eine Elasticsearch-Domain Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die Domain keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Domain mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen

möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Elasticsearch-Domain finden Sie unter Arbeiten mit Tags im Amazon OpenSearch Service Developer Guide.

EventBridge Amazon-Kontrollen

Diese Kontrollen beziehen sich auf EventBridge Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[EventBridge.2] EventBridge Eventbusse sollten gekennzeichnet sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Events::EventBus`

AWS Config Regel: `tagged-events-eventbus` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein EventBridge Amazon-Event-Bus Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Event-Bus keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Event-Bus mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem EventBridge Event-Bus finden Sie unter EventBridge Amazon-Tags im EventBridge Amazon-Benutzerhandbuch.

[EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden

Verwandte Anforderungen: NIST.800-53.R5 AC-2, NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-5, NIST.800-53.R5 AC-6, NIST.800-53.R5 R5 AC-6 (3)

Kategorie: Schützen > Sicheres Zugriffsmanagement > Konfiguration von Ressourcenrichtlinien

Schweregrad: Niedrig

Art der Ressource: `AWS::Events::EventBus`

AWS Config -Regel: `custom-schema-registry-policy-attached`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein EventBridge benutzerdefinierter Amazon Event Bus mit einer ressourcenbasierten Richtlinie verknüpft ist. Diese Steuerung schlägt fehl, wenn dem benutzerdefinierten Event-Bus keine ressourcenbasierte Richtlinie zugewiesen wurde.

Standardmäßig ist an einen EventBridge benutzerdefinierten Ereignisbus keine ressourcenbasierte Richtlinie angehängt. Dadurch können die Principals im Konto auf den Event-Bus zugreifen. Indem Sie eine ressourcenbasierte Richtlinie an den Event-Bus anhängen, können Sie den Zugriff auf den Event-Bus auf bestimmte Konten beschränken und Entitäten in einem anderen Konto bewusst Zugriff gewähren.

Abhilfe

Informationen zum Hinzufügen einer ressourcenbasierten Richtlinie zu einem EventBridge benutzerdefinierten Event-Bus finden Sie unter Verwaltung von Event-Bus-Berechtigungen im EventBridge Amazon-Benutzerhandbuch.

[EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::Events::Endpoint`

AWS Config -Regel: `global-endpoint-event-replication-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Ereignisreplikation für einen EventBridge globalen Amazon-Endpunkt aktiviert ist. Die Steuerung schlägt fehl, wenn die Ereignisreplikation für einen globalen Endpunkt nicht aktiviert ist.

Globale Endpunkte tragen dazu bei, dass Ihre Anwendung regional fehlertolerant ist. Zunächst weisen Sie dem Endpunkt eine Amazon-Route-53-Zustandsprüfung zu. Wenn ein Failover initiiert wird, meldet die Integritätsprüfung einen „fehlerhaften“ Zustand. Innerhalb weniger Minuten nach der Einleitung des Failovers werden alle benutzerdefinierten Ereignisse an einen Event Bus in der sekundären Region weitergeleitet und von diesem Event Bus verarbeitet. Wenn Sie globale Endpunkte verwenden, können Sie die Ereignisreplikation aktivieren. Bei der Ereignisreplikation werden alle benutzerdefinierten Ereignisse mithilfe verwalteter Regeln an die Event Buses in der primären und sekundären Region gesendet. Wir empfehlen, die Ereignisreplikation bei der Einrichtung globaler Endgeräte zu aktivieren. Mithilfe der Ereignisreplikation können Sie überprüfen, ob Ihre globalen Endpunkte korrekt konfiguriert sind. Für die automatische Wiederherstellung nach einem Failover-Ereignis ist die Ereignisreplikation erforderlich. Wenn Sie die Ereignisreplikation nicht aktiviert haben, müssen Sie die Route 53-Zustandsprüfung manuell auf „Fehlerfrei“ zurücksetzen, bevor Ereignisse zurück in die primäre Region umgeleitet werden.

> **Note**
>
> Wenn Sie benutzerdefinierte Ereignisbusse verwenden, benötigen Sie in jeder Region einen benutzerdefinierten geraden Bus mit demselben Namen und demselben Konto, damit der Failover ordnungsgemäß funktioniert. Wenn Sie die Ereignisreplikation aktivieren, können sich Ihre monatlichen Kosten erhöhen. Informationen zu den Preisen finden Sie unter EventBridge Amazon-Preise.

Abhilfe

Informationen zum Aktivieren der Ereignisreplikation für EventBridge globale Endgeräte finden Sie unter Erstellen eines globalen Endpunkts im EventBridge Amazon-Benutzerhandbuch. Wählen Sie für die Ereignisreplikation die Option Ereignisreplikation aktiviert aus.

Amazon FSx-Steuerelemente

Diese Kontrollen beziehen sich auf Amazon FSx-Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::FSx::FileSystem`

AWS Config -Regel: `fsx-openzfs-copy-tags-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon FSx for OpenZFS-Dateisystem so konfiguriert ist, dass es Tags auf Backups und Volumes kopiert. Die Kontrolle schlägt fehl, wenn das OpenZFS-Dateisystem nicht so konfiguriert ist, dass es Tags auf Backups und Volumes kopiert.

Die Identifizierung und Inventarisierung Ihrer IT-Ressourcen ist ein wichtiger Aspekt der Unternehmensführung und Sicherheit. Mithilfe von Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Dies ist nützlich, wenn Sie über viele Ressourcen desselben Typs verfügen, da Sie eine bestimmte Ressource anhand der Tags, die Sie ihr zugewiesen haben, schnell identifizieren können.

Abhilfe

Informationen zur Konfiguration eines FSx for OpenZFS-Dateisystems zum Kopieren von Tags auf Backups und Volumes finden Sie unter Aktualisieren eines Dateisystems im Amazon FSx OpenZFS-Benutzerhandbuch.

[FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden

Verwandte Anforderungen: NIST.800-53.R5 CP-9, NIST.800-53.R5 CM-8

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::FSx::FileSystem`

AWS Config -Regel: `fsx-lustre-copy-tags-to-backups`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon FSx for Lustre-Dateisystem so konfiguriert ist, dass es Tags auf Backups und Volumes kopiert. Die Kontrolle schlägt fehl, wenn das Lustre-Dateisystem nicht so konfiguriert ist, dass es Tags auf Backups und Volumes kopiert.

Die Identifizierung und Inventarisierung Ihrer IT-Ressourcen ist ein wichtiger Aspekt der Unternehmensführung und Sicherheit. Mithilfe von Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Dies ist nützlich, wenn Sie über viele Ressourcen desselben Typs verfügen, da Sie eine bestimmte Ressource anhand der Tags, die Sie ihr zugewiesen haben, schnell identifizieren können.

Abhilfe

Informationen zur Konfiguration eines FSx for Lustre-Dateisystems zum Kopieren von Tags in Backups finden Sie unter Aktualisieren eines Dateisystems im Amazon FSx OpenZFS-Benutzerhandbuch.

AWS Global Accelerator steuert

Diese Kontrollen beziehen sich auf die Ressourcen von Global Accelerator.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::GlobalAccelerator::Accelerator`

AWS Config Regel: `tagged-globalaccelerator-accelerator` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein AWS Global Accelerator Accelerator über Tags mit den spezifischen Tasten verfügt, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn der Beschleuniger keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Beschleuniger mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Global Accelerator Global Accelerator finden Sie unter Tagging in AWS Global Accelerator im AWS Global Accelerator Developer Guide.

AWS Glue Steuerungen

Diese Kontrollen beziehen sich auf AWS Glue Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Glue.1] AWS Glue Jobs sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Glue::Job`

AWS Config Regel: `tagged-glue-job` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein AWS Glue Job Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn der Job keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Job mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck,

Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Stichwörtern zu einem AWS Glue Job finden Sie unter AWS Stichwörter AWS Glue im AWS Glue Benutzerhandbuch.

GuardDuty Amazon-Kontrollen

Diese Kontrollen beziehen sich auf GuardDuty Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[GuardDuty.1] GuardDuty sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v3.2.1/11.4, NIST.800-53.R5 AC-2 (12), NIST.800-53.R5 AU-6 (1), NIST.800-53.R5 AU-6 (5), NIST.800-53.R5 CA-7, NIST.800-53.R5 CM-8 (3), NIST.800-53.R5 RA-3 (4), NIST.800-53.R5 SA-11 (1), NIST.800-53.R5 SA-11 (6), NIST.800-53.R5 SA-15 (2), NIST.800-53.R5 SA-15 (8), NIST.800-53.R5 SA-8 (19), NIST.800-53.R5 SA-8 (21), NIST.800-53.R5 SA-8 (25), NIST.800-53.R5 SC-5, NIST.800-53.R5 SC-5 (1), NIST.800-53.R5 SC-5 (3),

NIST.800-53.R5 SI-20, NIST.800-53.R5 SI-3 (8), NIst.800-53.R5 SI-4, NIst.800-53.R5 SI-4 (1), NIST.800-53.r5 SI-4 (13), NIST.800-53 .r5 SI-4 (2), NIST.800-53.r5 SI-4 (22), NIST.800-53.R5 SI-4 (25), NIST.800-53.r5 SI-4 (4), NIST.800-53.r5 SI-4 (5)

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `guardduty-enabled-centralized`

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob Amazon in Ihrem GuardDuty Konto und Ihrer Region aktiviert GuardDuty ist.

Es wird dringend empfohlen, die Aktivierung GuardDuty in allen unterstützten AWS Regionen durchzuführen. Auf diese Weise können GuardDuty Sie Erkenntnisse über nicht autorisierte oder ungewöhnliche Aktivitäten gewinnen, auch in Regionen, die Sie nicht aktiv nutzen. Dies ermöglicht auch GuardDuty die Überwachung globaler CloudTrail Ereignisse AWS-Services wie IAM.

Abhilfe

Um dieses Problem zu beheben, aktivieren Sie. GuardDuty

Einzelheiten zur Aktivierung GuardDuty, einschließlich der Verwendung AWS Organizations zur Verwaltung mehrerer Konten, finden Sie unter Erste Schritte mit GuardDuty im GuardDuty Amazon-Benutzerhandbuch.

[GuardDuty.2] GuardDuty Filter sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::GuardDuty::Filter`

AWS Config Regel: `tagged-guardduty-filter` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein GuardDuty Amazon-Filter Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn der Filter keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Filter mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem GuardDuty Filter finden Sie TagResourcein der Amazon GuardDuty API-Referenz.

[GuardDuty.3] GuardDuty IPSets sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::GuardDuty::IPSet`

AWS Config Regel: `tagged-guardduty-ipset` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein Amazon GuardDuty IPSet Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn das IPSet keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das IPSet mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem GuardDuty IPSet finden Sie TagResourcein der Amazon GuardDuty API-Referenz.

[GuardDuty.4] GuardDuty Detektoren sollten markiert werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::GuardDuty::Detector`

AWS Config Regel: `tagged-guardduty-detector` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Diese Steuerung prüft, ob ein GuardDuty Amazon-Detektor Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Detektor keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft die Steuerung nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Detektor mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem GuardDuty Detektor finden Sie TagResourcein der Amazon GuardDuty API-Referenz.

AWS Identity and Access Management steuert

Diese Kontrollen beziehen sich auf IAM-Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen

Verwandte Anforderungen: PCI DSS v3.2.1/7.2.1, CIS AWS Foundations Benchmark v1.2.0/1.22, CIS Foundations Benchmark v1.4.0/1.16, NIST.800-53.R5 AC-2, NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-5, NIST.800-53.R5 AC-6, NIST.800-53.R5 AC-6 (10), NIST.800-53.R5 AC-6 (2), NIST.800-53.R5 AC-6 (3) AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::IAM::Policy`

AWS Config -Regel: `iam-policy-no-statements-with-admin-access`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `excludePermissionBoundaryPolicy: true`(nicht anpassbar)

Dieses Steuerelement überprüft, ob die Standardversion der IAM-Richtlinien (auch als vom Kunden verwaltete Richtlinien bezeichnet) Administratorzugriff hat. Dazu wird eine Erklärung mit dem Zusatz „`"Effect": "Allow"`mit `"Action": "*"` über`"Resource": "*"`“ hinzugefügt. Die Kontrolle schlägt fehl, wenn Sie über IAM-Richtlinien mit einer solchen Erklärung verfügen.

Das Steuerelement prüft nur die vom Kunden verwalteten Richtlinien, die Sie erstellen. Inline-Richtlinien und AWS verwaltete Richtlinien werden nicht geprüft.

IAM-Richtlinien definieren eine Reihe von Rechten, die Benutzern, Gruppen oder Rollen gewährt werden. Gemäß den üblichen Sicherheitshinweisen wird AWS empfohlen, die geringsten Rechte zu gewähren, d. h., nur die Berechtigungen zu gewähren, die für die Ausführung einer Aufgabe erforderlich sind. Wenn Sie umfassende administrative Berechtigungen anstelle nur derjenigen bereitstellen, die der Benutzer für seine Tätigkeit benötigt, ermöglichen Sie unter Umständen ungewollte Aktionen mit den Ressourcen.

Anstatt umfassende administrative Berechtigungen zu gewähren, legen Sie fest, was Benutzer tun müssen, und erstellen Sie dann Richtlinien, mit denen die Benutzer nur diese Aufgaben ausführen können. Es ist sicherer, mit einem Mindestsatz von Berechtigungen zu beginnen und bei Bedarf zusätzliche Berechtigungen zu erteilen. Beginnen Sie nicht mit Berechtigungen, die zu weit gefasst sind, und versuchen Sie dann, sie später zu begrenzen.

Sie sollten IAM-Richtlinien entfernen, die eine Erklärung `"Effect": "Allow"` mit der Aufschrift `"Action": "*"` über `"Resource": "*"` enthalten.

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Informationen dazu, wie Sie Ihre IAM-Richtlinien so ändern, dass sie keine vollen „*“ -Administratorrechte gewähren, finden Sie unter Bearbeiten von IAM-Richtlinien im IAM-Benutzerhandbuch.

[IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

Verwandte Anforderungen: PCI DSS v3.2.1/7.2.1, CIS AWS Foundations Benchmark v3.0.0/1.15, CIS Foundations Benchmark v1.2.0/1.16, NIST.800-53.R5 AC-2, NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.R5 AC-6, NIST.800-53.R5 AC-6 (3) AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: `AWS::IAM::User`

AWS Config -Regel: `iam-user-no-policies-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Ihren IAM-Benutzern Richtlinien zugeordnet sind. Die Kontrolle schlägt fehl, wenn Ihren IAM-Benutzern Richtlinien zugewiesen sind. Stattdessen müssen IAM-Benutzer Berechtigungen von IAM-Gruppen erben oder eine Rolle übernehmen.

Standardmäßig haben IAM-Benutzer, -Gruppen und -Rollen keinen Zugriff auf Ressourcen. AWS IAM-Richtlinien gewähren Benutzern, Gruppen oder Rollen Rechte. Wir empfehlen, dass Sie IAM-Richtlinien direkt auf Gruppen und Rollen anwenden, jedoch nicht auf Benutzer. Das Zuweisen von Berechtigungen auf Gruppen- oder Rollenebene reduziert die Komplexität bei der Zugriffsverwaltung, wenn die Benutzeranzahl steigt. Eine Reduzierung der Komplexität bei der Zugriffsverwaltung kann wiederum das Risiko mindern, dass ein Prinzipal irrtümlicherweise übermäßige Berechtigungen erhält.

> **Note**
>
> Von Amazon Simple Email Service erstellte IAM-Benutzer werden automatisch mithilfe von Inline-Richtlinien erstellt. Security Hub nimmt diese Benutzer automatisch von dieser Kontrolle aus.

AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Um dieses Problem zu beheben, erstellen Sie eine IAM-Gruppe und hängen Sie die Richtlinie an die Gruppe an. Fügen Sie dann die Benutzer der Gruppe hinzu. Die Richtlinie gilt für jeden Benutzer in der Gruppe. Informationen zum Entfernen einer direkt mit einem Benutzer verknüpften Richtlinie finden Sie unter Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im IAM-Benutzerhandbuch.

[IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.14, CIS Foundations Benchmark v1.4.0/1.14, CIS AWS Foundations Benchmark v1.2.0/1.4, NIST.800-53.r5 AC-2 (1), AWS NIST.800-53.r5 AC-2 (3), NIST.800-53.r5 AC-3 (15)

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::IAM::User`

AWS Config -Regel: `access-keys-rotated`

Art des Zeitplans: Periodisch

Parameter:

- `maxAccessKeyAge`: `90` (nicht anpassbar)

Dieses Steuerelement prüft, ob die aktiven Zugriffsschlüssel innerhalb von 90 Tagen rotiert werden.

Wir empfehlen Ihnen dringend, nicht alle Zugriffsschlüssel in Ihrem Konto zu generieren und zu entfernen. Stattdessen empfiehlt es sich, entweder eine oder mehrere IAM-Rollen zu erstellen oder

den Verbund über AWS IAM Identity Center zu verwenden. Sie können diese Methoden verwenden, um Ihren Benutzern den Zugriff auf AWS Management Console und AWS CLI zu ermöglichen.

Jeder Ansatz hat seine Anwendungsfälle. Ein Verbund eignet sich im Allgemeinen besser für Unternehmen, die über ein vorhandenes zentrales Verzeichnis verfügen oder planen, mehr als die aktuelle Anzahl an IAM-Benutzern zu benötigen. Anwendungen, die außerhalb einer AWS Umgebung ausgeführt werden, benötigen Zugriffstasten für den programmatischen Zugriff AWS auf Ressourcen.

Wenn die Ressourcen, die programmatischen Zugriff benötigen, jedoch intern ausgeführt werden AWS, empfiehlt es sich, IAM-Rollen zu verwenden. Rollen ermöglichen es Ihnen, einer Ressource Zugriff zu gewähren, ohne eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel in die Konfiguration zu integrieren.

Weitere Informationen zum Schutz Ihrer Zugriffsschlüssel und Ihres Kontos finden Sie unter Bewährte Methoden für die Verwaltung von AWS Zugriffsschlüsseln in der. Allgemeine AWS-Referenz Lesen Sie auch den Blogbeitrag Richtlinien für Ihren Schutz AWS-Konto bei der Verwendung von programmatischem Zugriff.

Wenn Sie bereits über einen Zugriffsschlüssel verfügen, empfiehlt Security Hub, die Zugangsschlüssel alle 90 Tage zu wechseln. Das Rotieren von Zugriffsschlüsseln reduziert die Gefahr, dass ein Zugriffsschlüssel eines kompromittierten oder gesperrten Kontos verwendet werden kann. Außerdem wird sichergestellt, dass mit einem alten Schlüssel, der möglicherweise verloren gegangen ist, geknackt bzw. gestohlen wurde, nicht auf Daten zugegriffen werden kann. Aktualisieren Sie Ihre Anwendungen immer, nachdem Sie Zugriffsschlüssel rotiert haben.

Zugriffsschlüssel bestehen aus einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel. Sie werden verwendet, um programmatische Anfragen zu signieren, die Sie stellen AWS. Benutzer benötigen ihre eigenen Zugriffsschlüssel, um programmgesteuerte Aufrufe AWS von den Tools for Windows AWS CLI PowerShell, den AWS SDKs oder direkte HTTP-Aufrufe mithilfe der API-Operationen für einzelne Benutzer zu tätigen. AWS-Services

Wenn Ihre Organisation AWS IAM Identity Center (IAM Identity Center) verwendet, können sich Ihre Benutzer bei Active Directory, einem integrierten IAM Identity Center-Verzeichnis oder einem anderen Identitätsanbieter (IdP) anmelden, der mit IAM Identity Center verbunden ist. Sie können dann einer IAM-Rolle zugeordnet werden, die es ihnen ermöglicht, AWS CLI Befehle auszuführen oder AWS API-Operationen aufzurufen, ohne dass Zugriffsschlüssel erforderlich sind. Weitere Informationen finden Sie im AWS Command Line Interface Benutzerhandbuch unter Konfiguration der AWS CLI zu AWS IAM Identity Center verwendenden.

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Informationen zur Rotation von Zugriffsschlüsseln, die älter als 90 Tage sind, finden Sie unter Rotieren von Zugriffsschlüsseln im IAM-Benutzerhandbuch. Folgen Sie den Anweisungen für alle Benutzer, deren Zugriffsschlüssel älter als 90 Tage ist.

[IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.4, CIS Foundations Benchmark v1.4.0/1.4, CIS AWS Foundations Benchmark v1.2.0/1.12, PCI DSS v3.2.1/2.1, PCI DSS v3.2.1/7.2.1, NIST.800-53.R5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (15) (7), NIST.800-53.R5 AC-6, NIST.800-53.R5 AC-6 (10), NIST.800-53.R5 AC-6 (2) AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Kritisch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-root-access-key-check`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob der Root-Benutzerzugriffsschlüssel vorhanden ist.

Der Root-Benutzer ist der Benutzer mit den meisten Rechten in einem AWS-Konto. AWS Zugriffstasten ermöglichen den programmatischen Zugriff auf ein bestimmtes Konto.

Security Hub empfiehlt, dass Sie alle Zugriffsschlüssel entfernen, die dem Root-Benutzer zugeordnet sind. Dies schränkt die Vektoren ein, die verwendet werden können, um Ihr Konto zu gefährden.

Darüber hinaus fördert es die Erstellung und Verwendung rollenbasierter Konten nach dem Prinzip der minimalen Rechte.

Abhilfe

Informationen zum Löschen des Root-Benutzerzugriffsschlüssels finden Sie unter Löschen von Zugriffsschlüsseln für den Root-Benutzer im IAM-Benutzerhandbuch. Informationen zum Löschen der Root-Benutzerzugriffsschlüssel aus einem AWS-Konto IN AWS GovCloud (US) finden Sie unter Löschen der Root-Benutzerzugriffsschlüssel für mein AWS GovCloud (US) Konto im AWS GovCloud (US) Benutzerhandbuch.

[IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.10, CIS AWS Foundations Benchmark v1.4.0/1.10, CIS Foundations Benchmark v1.2.0/1.2, NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 IA-2 (1), NIST.800-53.r5 IA-2 (2), NIST.800-53.r5 IA-2 (2) 2 (6), NIST.800-53.R5 IA-2 (8) AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::IAM::User`

AWS Config -Regel: `mfa-enabled-for-iam-console-access`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die AWS Multi-Faktor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist, die ein Konsolenkennwort verwenden.

Multi-Factor Authentication (MFA) bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Wenn MFA aktiviert ist, wird ein Benutzer, wenn er sich AWS auf einer Website anmeldet, nach seinem Benutzernamen und Passwort gefragt. Darüber hinaus werden sie von ihrem AWS MFA-Gerät zur Eingabe eines Authentifizierungscodes aufgefordert.

Es wird empfohlen, MFA für alle Konten zu aktivieren, die über ein Konsolenpasswort verfügen. MFA wurde entwickelt, um mehr Sicherheit für den Konsolenzugriff zu bieten. Der authentifizierende

Prinzipal muss über ein Gerät verfügen, das einen zeitkritischen Schlüssel ausgibt und Kenntnisse über Anmeldeinformationen haben muss.

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Informationen zum Hinzufügen von MFA für IAM-Benutzer finden Sie unter Verwenden der Multi-Faktor-Authentifizierung (MFA) AWS im IAM-Benutzerhandbuch.

Wir bieten berechtigten Kunden einen kostenlosen MFA-Sicherheitsschlüssel an. Prüfen Sie, ob Sie sich qualifizieren, und bestellen Sie Ihren kostenlosen Schlüssel.

[IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.6, CIS AWS Foundations Benchmark v1.4.0/1.6, CIS Foundations Benchmark v1.2.0/1.14, PCI DSS v3.2.1/8.3.1, NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 IA-2 (2), NIST.800-53.R5 IA-2 (6), NIST.800-53.R5 IA-2 (8) AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Kritisch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `root-account-hardware-mfa-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Sie AWS-Konto für die Verwendung eines Hardware-Geräts mit Multi-Faktor-Authentifizierung (MFA) aktiviert sind, um sich mit Root-Benutzeranmeldedaten anzumelden.

Die Steuerung schlägt fehl, wenn MFA nicht aktiviert ist oder wenn virtuelle MFA-Geräte sich mit Root-Benutzeranmeldedaten anmelden dürfen.

Eine virtuelle MFA bietet möglicherweise nicht das gleiche Sicherheitsniveau wie ein Hardware-MFA-Gerät. Es wird empfohlen, dass Sie nur ein virtuelles MFA-Gerät verwenden, während Sie auf die Genehmigung des Hardware-Kaufs oder auf die Ankunft Ihrer Hardware warten. Weitere Informationen finden Sie unter Aktivieren eines Geräts (Konsole) mit virtueller Multi-Faktor-Authentifizierung (MFA) im IAM-Benutzerhandbuch.

Sowohl zeitbasierte Einmalkennwörter (TOTP) als auch Universal 2nd Factor (U2F) -Token eignen sich als Hardware-MFA-Optionen.

Abhilfe

Informationen zum Hinzufügen eines Hardware-MFA-Geräts für den Root-Benutzer finden Sie unter Aktivieren eines Hardware-MFA-Geräts für den AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Wir bieten berechtigten Kunden einen kostenlosen MFA-Sicherheitsschlüssel an. Prüfen Sie, ob Sie sich qualifizieren, und bestellen Sie Ihren kostenlosen Schlüssel.

[IAM.7] Die Passwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-2 (3), NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 IA-5 (1)

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`RequireUppercaseCharacters`	Das Passwort muss mindestens einen Großbuchstaben enthalten	Boolesch	`true` oder `false`	`true`
`RequireLowercaseCharacters`	Das Passwort muss mindestens einen Kleinbuchstaben enthalten	Boolesch	`true` oder `false`	`true`
`RequireSymbols`	Das Passwort muss mindestens ein Symbol enthalten	Boolesch	`true` oder `false`	`true`
`RequireNumbers`	Das Passwort muss mindestens eine Zahl enthalten	Boolesch	`true` oder `false`	`true`
`MinimumPasswordLength`	Mindestanzahl von Zeichen im Passwort	Ganzzahl	`8` auf `128`	`8`
`PasswordReusePrevention`	Anzahl der Passwortrotationen, bevor ein altes Passwort wiederverwendet werden kann	Ganzzahl	`12` auf `24`	Kein Standardwert
`MaxPasswordAge`	Anzahl der Tage bis zum Ablauf des Passworts	Ganzzahl	`1` auf `90`	Kein Standardwert

Dieses Steuerelement prüft, ob die Kontopasswortrichtlinie für IAM-Benutzer starke Konfigurationen verwendet. Die Steuerung schlägt fehl, wenn die Kennwortrichtlinie keine starken Konfigurationen verwendet. Sofern Sie keine benutzerdefinierten Parameterwerte angeben, verwendet Security Hub die in der vorherigen Tabelle genannten Standardwerte. Die `MaxPasswordAge` Parameter `PasswordReusePrevention` und haben keinen Standardwert. Wenn Sie diese Parameter

ausschließen, ignoriert Security Hub bei der Auswertung dieser Steuerung die Anzahl der Kennwortrotationen und das Kennwortalter.

Für den Zugriff auf AWS Management Console benötigen IAM-Benutzer Passwörter. Als bewährte Methode empfiehlt Security Hub dringend, anstelle der Erstellung von IAM-Benutzern den Verbund zu verwenden. Mit dem Verbund können sich Benutzer mit ihren vorhandenen Unternehmensanmeldeinformationen bei der AWS Management Console anmelden. Verwenden Sie AWS IAM Identity Center (IAM Identity Center), um den Benutzer zu erstellen oder zu verbinden, und übernehmen Sie dann eine IAM-Rolle für ein Konto.

Weitere Informationen zu Identitätsanbietern und Verbund finden Sie unter Identitätsanbieter und Verbund im IAM-Benutzerhandbuch. Weitere Informationen zu IAM Identity Center finden Sie im AWS IAM Identity Center Benutzerhandbuch.

Wenn Sie IAM-Benutzer verwenden müssen, empfiehlt Security Hub, die Erstellung sicherer Benutzerkennwörter zu erzwingen. Sie können auf Ihrem Computer eine Passwortrichtlinie einrichten AWS-Konto , um die Komplexitätsanforderungen und die obligatorischen Rotationsperioden für Passwörter festzulegen. Wenn Sie eine Kennwortrichtlinie erstellen oder ändern, werden die meisten Einstellungen der Kennwortrichtlinie durchgesetzt, wenn Benutzer ihre Passwörter das nächste Mal ändern. Einige Einstellungen werden sofort durchgesetzt.

Abhilfe

Informationen zur Aktualisierung Ihrer Kennwortrichtlinie finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch.

[IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden

Verwandte Anforderungen: PCI DSS v3.2.1/8.1.4, CIS AWS Foundations Benchmark v1.2.0/1.3, NIST.800-53.R5 AC-2, NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-2 (3), NIST.800-53.R5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.R5 AC-6

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::IAM::User`

AWS Config -Regel: `iam-user-unused-credentials-check`

Art des Zeitplans: Periodisch

Parameter:

- `maxCredentialUsageAge`: `90` (nicht anpassbar)

Dieses Steuerelement prüft, ob Ihre IAM-Benutzer über Passwörter oder aktive Zugriffsschlüssel verfügen, die seit 90 Tagen nicht verwendet wurden.

IAM-Benutzer können mit verschiedenen Arten von Anmeldeinformationen wie Passwörtern oder Zugriffsschlüsseln auf AWS Ressourcen zugreifen.

Security Hub empfiehlt, alle Anmeldeinformationen zu entfernen oder zu deaktivieren, die 90 Tage oder länger nicht verwendet wurden. Durch das Deaktivieren oder Entfernen unnötiger Anmeldeinformationen reduzieren Sie den möglichen Schaden, der mit den Anmeldeinformationen eines kompromittierten oder ungenutzten Kontos angerichtet werden kann.

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Wenn Sie Benutzerinformationen in der IAM-Konsole anzeigen, gibt es Spalten für das Alter des Zugriffsschlüssels, das Alter des Kennworts und die letzte Aktivität. Wenn der Wert in einer dieser Spalten mehr als 90 Tage beträgt, sollten Sie die Anmeldeinformationen für diese Benutzer deaktivieren.

Sie können auch Berichte mit Anmeldeinformationen verwenden, um Benutzer zu überwachen und Benutzer zu identifizieren, die 90 oder mehr Tage lang keine Aktivität mehr hatten. Sie können Berichte über Anmeldeinformationen im `.csv` Format von der IAM-Konsole herunterladen.

Nachdem Sie die inaktiven Konten oder ungenutzten Anmeldeinformationen identifiziert haben, deaktivieren Sie sie. Anweisungen finden Sie im IAM-Benutzerhandbuch unter Erstellen, Ändern oder Löschen eines IAM-Benutzerkennworts (Konsole).

[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein

Verwandte Anforderungen: PCI DSS v3.2.1/8.3.1, CIS AWS Foundations Benchmark v3.0.0/1.5, CIS Foundations Benchmark v1.4.0/1.5, CIS AWS Foundations Benchmark v1.2.0/1.13, NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 IA-2 (2), NIST.800-53.R5 IA-2 (6), NIST.800-53.R5 IA-2 (8) AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Kritisch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `root-account-mfa-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Der Root-Benutzer hat vollständigen Zugriff auf alle Dienste und Ressourcen in einem AWS-Konto. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Wenn MFA aktiviert ist, wird ein Benutzer bei der Anmeldung bei der aufgefordert AWS Management Console, seinen Benutzernamen und sein Passwort sowie einen Authentifizierungscode von seinem AWS MFA-Gerät einzugeben.

Wenn Sie Virtual MFA für den Root-Benutzer verwenden, empfiehlt CIS, dass es sich bei dem verwendeten Gerät nicht um ein persönliches Gerät handelt. Verwenden Sie stattdessen ein dediziertes Mobilgerät (Tablet oder Smartphone), das Sie verwalten und für das Sie dafür sorgen, dass es unabhängig von persönlichen Geräten geladen und abgesichert wird. Dies mindert das Risiko, den Zugriff auf die MFA zu verlieren, weil das Gerät verloren geht, eingetauscht wird oder der Mitarbeiter, dem das Gerät gehört, nicht mehr im Unternehmen beschäftigt ist,

Abhilfe

Informationen zur Aktivierung von MFA für den Root-Benutzer finden Sie unter MFA für den AWS-Konto Root-Benutzer aktivieren im Referenzhandbuch zur AWS Kontoverwaltung.

[IAM.10] Passwortrichtlinien für IAM-Benutzer sollten strenge Laufzeiten haben AWS Config

Verwandte Anforderungen: PCI DSS v3.2.1/8.1.4, PCI DSS v3.2.1/8.2.3, PCI DSS v3.2.1/8.2.4, PCI DSS v3.2.1/8.2.5

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die Kontopasswortrichtlinie für IAM-Benutzer die folgenden PCI-DSS-Mindestkonfigurationen verwendet.

- `RequireUppercaseCharacters`— Das Passwort muss mindestens einen Großbuchstaben enthalten. (Standardwert = `true`)
- `RequireLowercaseCharacters`— Das Passwort muss mindestens einen Kleinbuchstaben enthalten. (Standardwert = `true`)
- `RequireNumbers`— Erfordert mindestens eine Zahl im Passwort. (Standardwert = `true`)
- `MinimumPasswordLength`— Mindestlänge des Passworts. (Standard = 7 oder länger)
- `PasswordReusePrevention`— Anzahl der Passwörter vor der Wiederverwendung. (Standard = 4)
- MaxPasswordAge — Anzahl der Tage bis zum Ablauf des Passworts. (Standard = 90)

Abhilfe

Informationen zur Aktualisierung Ihrer Kennwortrichtlinie zur Verwendung der empfohlenen Konfiguration finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch.

[IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert

Verwandte Anforderungen: CIS Foundations Benchmark v1.2.0/1.5 AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter: Keine

Passwortrichtlinien erzwingen zum Teil Anforderungen in Zusammenhang mit der Passwortkomplexität. Verwenden Sie IAM-Passwortrichtlinien, um sicherzustellen, dass Passwörter unterschiedliche Zeichensätze verwenden.

CIS empfiehlt, dass die Kennwortrichtlinie mindestens einen Großbuchstaben erfordert. Die Festlegung einer Richtlinie für die Passwortkomplexität steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch. Wählen Sie unter Passwortstärke die Option Mindestens einen Großbuchstaben des lateinischen Alphabets erforderlich (A—Z) aus.

[IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert

Verwandte Anforderungen: CIS Foundations Benchmark v1.2.0/1.6 AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter: Keine

Passwortrichtlinien erzwingen zum Teil Anforderungen in Zusammenhang mit der Passwortkomplexität. Verwenden Sie IAM-Passwortrichtlinien, um sicherzustellen, dass Passwörter

unterschiedliche Zeichensätze verwenden. CIS empfiehlt, dass die Kennwortrichtlinie mindestens einen Kleinbuchstaben erfordert. Die Festlegung einer Richtlinie für die Passwortkomplexität steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch. Wählen Sie unter Passwortstärke die Option Mindestens einen Kleinbuchstaben des lateinischen Alphabets erforderlich (A—Z) aus.

[IAM.13] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist

Verwandte Anforderungen: CIS Foundations Benchmark v1.2.0/1.7 AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter: Keine

Passwortrichtlinien erzwingen zum Teil Anforderungen in Zusammenhang mit der Passwortkomplexität. Verwenden Sie IAM-Passwortrichtlinien, um sicherzustellen, dass Passwörter unterschiedliche Zeichensätze verwenden.

CIS empfiehlt, dass für die Kennwortrichtlinie mindestens ein Symbol erforderlich ist. Die Festlegung einer Richtlinie für die Passwortkomplexität steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch. Wählen Sie unter Passwortstärke die Option Mindestens ein nichtalphanumerisches Zeichen erforderlich aus.

[IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert

Verwandte Anforderungen: CIS Foundations Benchmark v1.2.0/1.8 AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter: Keine

Passwortrichtlinien erzwingen zum Teil Anforderungen in Zusammenhang mit der Passwortkomplexität. Verwenden Sie IAM-Passwortrichtlinien, um sicherzustellen, dass Passwörter unterschiedliche Zeichensätze verwenden.

CIS empfiehlt, dass für die Kennwortrichtlinie mindestens eine Zahl erforderlich ist. Die Festlegung einer Richtlinie für die Passwortkomplexität steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch. Wählen Sie unter Passwortstärke die Option Mindestens eine Zahl erforderlich aus.

[IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.8, CIS Foundations Benchmark v1.4.0/1.8, CIS AWS Foundations Benchmark v1.2.0/1.9 AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter: Keine

Passwortrichtlinien erzwingen zum Teil Anforderungen in Zusammenhang mit der Passwortkomplexität. Verwenden Sie IAM-Passwortrichtlinien, um sicherzustellen, dass Passwörter mindestens eine bestimmte Länge haben.

CIS empfiehlt, dass die Kennwortrichtlinie eine Mindestkennwortlänge von 14 Zeichen vorschreibt. Die Festlegung einer Richtlinie für die Passwortkomplexität steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch. Geben Sie für die Mindestlänge des Kennworts eine **14** oder eine größere Zahl ein.

[IAM.16] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.9, CIS Foundations Benchmark v1.4.0/1.9, CIS AWS Foundations Benchmark v1.2.0/1.10 AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement überprüft, ob die Anzahl der Passwörter, die Sie sich merken müssen, auf 24 gesetzt ist. Die Steuerung schlägt fehl, wenn der Wert nicht 24 ist.

IAM-Passwortrichtlinien können die Wiederverwendung eines bestimmten Passworts durch denselben Benutzer verhindern.

CIS empfiehlt, dass die Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert. Das Verhindern der Wiederverwendung von Passwörtern steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch. Geben Sie für „Wiederverwendung von Passwörtern verhindern“ ein. **24**

[IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft

Verwandte Anforderungen: CIS Foundations Benchmark v1.2.0/1.11 AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-password-policy`

Art des Zeitplans: Periodisch

Parameter: Keine

IAM-Passwortrichtlinien können vorschreiben, dass Passwörter nach einer bestimmten Anzahl von Tagen ausgetauscht werden oder abgelaufen sind.

CIS empfiehlt, dass die Kennwortrichtlinie Passwörter nach 90 Tagen oder weniger abläuft. Das Reduzieren der Lebensdauer von Passwörtern steigert die Widerstandskraft eines Kontos gegen Brute-Force-Anmeldeversuche. Darüber hinaus ist es in folgenden Situationen hilfreich, wenn regelmäßige Passwortänderungen gefordert werden:

- Passwörter können ohne Ihr Wissen gestohlen oder kompromittiert werden. Dies kann durch eine Systemkompromittierung, eine Softwareschwachstelle oder eine interne Bedrohung erfolgen.
- Bestimmte Web-Filter oder Proxy-Server von Unternehmen und Behörden können Datenverkehr abfangen und erfassen, selbst wenn er verschlüsselt ist.

- Viele Menschen verwenden dasselbe Passwort für viele Systeme, z. B. für die Arbeit, E-Mails und den privaten Gebrauch.
- Auf kompromittierten Endbenutzer-Workstations kann ein Keylogger vorhanden sein.

Abhilfe

Informationen zum Ändern Ihrer Kennwortrichtlinie finden Sie unter Einrichten einer Kontokennwortrichtlinie für IAM-Benutzer im IAM-Benutzerhandbuch. Geben Sie für „Ablauf des Kennworts aktivieren“ eine kleinere **`90`** Zahl oder ein.

[IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.17, CIS Foundations Benchmark v1.4.0/1.17, CIS AWS Foundations Benchmark v1.2.0/1.20 AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `iam-policy-in-use`

Art des Zeitplans: Periodisch

Parameter:

- `policyARN`: `arn:`*`partition`*`:iam::aws:policy/AWSSupportAccess` (nicht anpassbar)
- `policyUsageType`: `ANY` (nicht anpassbar)

AWS bietet ein Support-Center, das für die Benachrichtigung und Reaktion auf Vorfälle sowie für technischen Support und Kundendienst genutzt werden kann.

Erstellen Sie eine IAM-Rolle, damit autorisierte Benutzer Vorfälle mit AWS Support verwalten können. Durch die Implementierung von Least-Privilegien für die Zugriffskontrolle erfordert eine IAM-Rolle eine entsprechende IAM-Richtlinie, die den Zugriff auf das Supportcenter ermöglicht, damit Vorfälle bearbeitet werden können. AWS Support

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Um dieses Problem zu beheben, erstellen Sie eine Rolle, die es autorisierten Benutzern ermöglicht, AWS Support Vorfälle zu verwalten.

Um die Rolle zu erstellen, die für AWS Support den Zugriff verwendet werden soll

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im IAM-Navigationsbereich Rollen und anschließend Rolle erstellen aus.
3. Wählen Sie als Rollentyp die Option Andere AWS-Konto aus.
4. Geben Sie unter Konto-ID die AWS-Konto ID der AWS-Konto Person ein, der Sie Zugriff auf Ihre Ressourcen gewähren möchten.

   Wenn sich die Benutzer oder Gruppen, die diese Rolle übernehmen, im selben Konto befinden, geben Sie die lokale Kontonummer ein.

   > **Note**
   >
   > Der Administrator des angegebenen Kontos kann die Berechtigung erteilen, diese Rolle für alle -Benutzer in diesem Konto zu übernehmen. Hierzu fügt der Administrator eine Richtlinie an den Benutzer oder eine Gruppe an, mit der die Berechtigung für die Aktion `sts:AssumeRole` gewährt wird. In dieser Richtlinie muss die Ressource der Rollen-ARN sein.

5. Wählen Sie Weiter: Berechtigungen aus.
6. Suchen Sie nach der verwalteten Richtlinie `AWSSupportAccess`.
7. Wählen Sie das Kontrollkästchen für die verwaltete `AWSSupportAccess`-Richtlinie aus.
8. Wählen Sie Weiter: Markierungen.

9. (Optional) Um der Rolle Metadaten hinzuzufügen, fügen Sie Tags als Schlüssel-Wert-Paare hinzu.

   Weitere Informationen zur Verwendung von Tags in IAM finden Sie unter Tagging von IAM-Benutzern und -Rollen im IAM-Benutzerhandbuch.
10. Klicken Sie auf Next: Review (Weiter: Prüfen).
11. Geben Sie unter Role name (Rollenname) einen Namen für Ihre Rolle ein.

    Rollennamen müssen innerhalb Ihrer eindeutig sein. AWS-Konto Sie unterscheiden nicht zwischen Groß- und Kleinschreibung.
12. (Optional) Geben Sie im Feld Role description (Rollenbeschreibung) eine Beschreibung für die neue Rolle ein.
13. Prüfen Sie die Rolle und klicken Sie dann auf Create role (Rolle erstellen).

[IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein

Verwandte Anforderungen: PCI DSS v3.2.1/8.3.1, NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 IA-2 (1), NIST.800-53.R5 IA-2 (2), NIST.800-53.R5 IA-2 (6), NIST.800-53.R5 IA-2 (8))

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::IAM::User`

AWS Config -Regel: `iam-user-mfa-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die IAM-Benutzer die Multi-Faktor-Authentifizierung (MFA) aktiviert haben.

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese

Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Informationen zum Hinzufügen von MFA für IAM-Benutzer finden Sie unter Aktivieren von MFA-Geräten für Benutzer AWS im IAM-Benutzerhandbuch.

[IAM.20] Vermeiden Sie die Verwendung des Root-Benutzers

Important

Security Hub hat diese Kontrolle im April 2024 eingestellt. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: CIS AWS Foundations Benchmark v1.2.0/1.1

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: `AWS::IAM::User`

AWS Config Regel: `use-of-root-account-test` (benutzerdefinierte Security Hub Hub-Regel)

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob für an AWS-Konto Beschränkungen für die Nutzung des Root-Benutzers gelten. Das Steuerelement bewertet die folgenden Ressourcen:

- Amazon Simple Notification Service (Amazon SNS)-Themen
- AWS CloudTrail Pfade
- Mit den CloudTrail Pfaden verknüpfte metrische Filter
- CloudWatch Amazon-Alarme basierend auf den Filtern

Bei dieser Prüfung wird `FAILED` festgestellt, ob eine oder mehrere der folgenden Aussagen zutreffen:

- Auf dem Konto sind keine CloudTrail Spuren vorhanden.
- Ein CloudTrail Trail ist aktiviert, aber nicht mit mindestens einem Trail für mehrere Regionen konfiguriert, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst.
- Ein CloudTrail Trail ist aktiviert, aber keiner CloudWatch Logs-Protokollgruppe zugeordnet.
- Der vom Center for Internet Security (CIS) vorgeschriebene exakte metrische Filter wird nicht verwendet. Der vorgeschriebene metrische Filter ist `'{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}'`.
- In dem Konto sind keine CloudWatch Alarme vorhanden, die auf dem metrischen Filter basieren.
- CloudWatch Alarme, die so konfiguriert sind, dass sie Benachrichtigungen an das zugehörige SNS-Thema senden, werden nicht aufgrund der Alarmbedingung ausgelöst.
- Das SNS-Thema entspricht nicht den Einschränkungen für das Senden einer Nachricht an ein SNS-Thema.
- Das SNS-Thema hat nicht mindestens einen Abonnenten.

Diese Prüfung führt zu einem Kontrollstatus, der `NO_DATA` angibt, ob eine oder mehrere der folgenden Aussagen zutreffen:

- Ein Trail mit mehreren Regionen befindet sich in einer anderen Region. Security Hub kann nur Ergebnisse in der Region generieren, in der sich der Trail befindet.
- Ein Trail mit mehreren Regionen gehört zu einem anderen Konto. Security Hub kann nur Ergebnisse für das Konto generieren, dem der Trail gehört.

Diese Prüfung führt zu einem Kontrollstatus, der `WARNING` angibt, ob eine oder mehrere der folgenden Aussagen zutreffen:

- Das aktuelle Konto ist nicht Eigentümer des SNS-Themas, auf das in der CloudWatch Warnung verwiesen wird.
- Das Girokonto hat beim Aufrufen der SNS-API keinen Zugriff auf das SNS-Thema. `ListSubscriptionsByTopic`

> **Note**
>
> Wir empfehlen, Organization Trails zu verwenden, um Ereignisse von vielen Konten in einer Organisation zu protokollieren. Organisationspfade sind standardmäßig regionsübergreifend

und können nur mit dem AWS Organizations Verwaltungskonto oder dem CloudTrail delegierten Administratorkonto verwaltet werden. Die Verwendung eines Organisationspfads führt zu einem Kontrollstatus von NO_DATA für Kontrollen, die in den Konten von Organisationsmitgliedern ausgewertet wurden. In Mitgliedskonten generiert Security Hub nur Ergebnisse für Ressourcen, die Mitgliedern gehören. Ergebnisse, die sich auf Organisationspfade beziehen, werden im Konto des Ressourcenbesitzers generiert. Sie können diese Ergebnisse in Ihrem delegierten Security Hub-Administratorkonto einsehen, indem Sie die regionsübergreifende Aggregation verwenden.

Es hat sich bewährt, Ihre Root-Benutzeranmeldedaten nur dann zu verwenden, wenn dies für die Konto- und Serviceverwaltung erforderlich ist. Wenden Sie IAM-Richtlinien direkt auf Gruppen und Rollen an, jedoch nicht auf Benutzer. Anweisungen zur Einrichtung eines Administrators für den täglichen Gebrauch finden Sie im IAM-Benutzerhandbuch unter Erstellen Ihres ersten IAM-Admin-Benutzers und Ihrer ersten Gruppe.

Abhilfe

Zu den Schritten zur Behebung dieses Problems gehören die Einrichtung eines Amazon SNS SNS-Themas, eines CloudTrail Trails, eines Metrikfilters und eines Alarms für den Metrikfilter.

Erstellen eines Amazon SNS-Themas

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Erstellen Sie ein Amazon SNS SNS-Thema, das alle CIS-Alarme empfängt.

   Erstellen Sie mindestens einen Abonnenten für das Thema. Weitere Informationen finden Sie unter Erste Schritte mit Amazon SNS im Benutzerhandbuch für Amazon Simple Notification Service.

Richten Sie als Nächstes eine aktive Option ein CloudTrail , die für alle Regionen gilt. Um dies zu tun, befolgen Sie die Schritte in the section called “[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst”.

Notieren Sie sich den Namen der Protokollgruppe CloudWatch Logs, die Sie dem CloudTrail Trail zuordnen. Sie erstellen den Metrikfilter für diese Protokollgruppe.

Erstellen Sie abschließend den metrischen Filter und den Alarm.

Erstellen eines Metrikfilters und Alarms

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Protokollgruppen aus.
3. Aktivieren Sie das Kontrollkästchen für die Protokollgruppe CloudWatch Logs, die dem von Ihnen erstellten CloudTrail Trail zugeordnet ist.
4. Wählen Sie unter Aktionen die Option Metrikfilter erstellen aus.
5. Gehen Sie unter Muster definieren wie folgt vor:

   a. Kopieren Sie das folgende Muster und fügen Sie es dann in das Feld Filter Pattern (Filtermuster) ein.

   ```
   {$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS &&
    $.eventType !="AwsServiceEvent"}
   ```

   b. Wählen Sie Weiter aus.
6. Gehen Sie unter Metrik zuweisen wie folgt vor:

   a. Geben Sie im Feld Filtername einen Namen für Ihren Metrikfilter ein.

   b. Geben **`LogMetrics`** Sie für Metric Namespace den Wert ein.

   Wenn Sie denselben Namespace für alle Ihre CIS-Log-Metrikfilter verwenden, werden alle CIS-Benchmark-Metriken zusammen gruppiert.

   c. Geben Sie unter Metrikname einen Namen für die Metrik ein. Merken Sie sich den Namen der Metrik. Sie müssen die Metrik auswählen, wenn Sie den Alarm erstellen.

   d. Geben Sie für Metric value (Metrikwert) **1** ein.

   e. Wählen Sie Weiter aus.
7. Überprüfen Sie unter Überprüfen und erstellen die Informationen, die Sie für den neuen Metrikfilter angegeben haben. Wählen Sie dann Metrikfilter erstellen aus.
8. Wählen Sie im Navigationsbereich Protokollgruppen und dann den Filter aus, den Sie unter Metrikfilter erstellt haben.
9. Aktivieren Sie das Kontrollkästchen für den Filter. Wählen Sie Alarm erstellen aus.
10. Gehen Sie unter Metrik und Bedingungen angeben wie folgt vor:

    a. Wählen Sie unter Bedingungen für Schwellenwert die Option Statisch aus.

    b. Wählen Sie unter Alarmbedingung definieren die Option Größer/Gleich aus.

c. Geben Sie unter Schwellenwert definieren den Wert ein. **1**

d. Wählen Sie Weiter aus.

11. Gehen Sie unter Aktionen konfigurieren wie folgt vor:

a. Wählen Sie unter Auslöser für den Alarmstatus die Option Bei Alarm aus.

b. Wählen Sie unter Select an SNS topic (SNS-Thema auswählen) die Option Select an existing SNS topic (Vorhandenes SNS-Thema auswählen) aus.

c. Geben Sie unter Benachrichtigung senden an den Namen des SNS-Themas ein, das Sie im vorherigen Verfahren erstellt haben.

d. Wählen Sie Weiter aus.

12. Geben Sie unter Namen und Beschreibung hinzufügen einen Namen und eine Beschreibung für den Alarm ein, z. B. **`CIS-1.1-RootAccountUsage`** Wählen Sie anschließend Weiter.

13. Überprüfen Sie unter Vorschau und Erstellung die Alarmkonfiguration. Wählen Sie anschließend Create alarm (Alarm erstellen) aus.

[IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen

Verwandte Anforderungen: NIST.800-53.R5 AC-2, NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-5, NIST.800-53.R5 AC-6, NIST.800-53.R5 R5 AC-6 (10), NIST.800-53.R5 AC-6 (2), NIST.800-53.R5 AC-6 (3)

Kategorie: Erkennen > Sicheres Zugriffsmanagement

Schweregrad: Niedrig

Art der Ressource: `AWS::IAM::Policy`

AWS Config -Regel: `iam-policy-no-statements-with-full-access`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `excludePermissionBoundaryPolicy`: `True` (nicht anpassbar)

Dieses Steuerelement prüft, ob die identitätsbasierten IAM-Richtlinien, die Sie erstellen, über Allow-Anweisungen verfügen, die den Platzhalter „*“ verwenden, um Berechtigungen für alle Aktionen in

einem Dienst zu gewähren. Das Steuerelement schlägt fehl, wenn eine Richtlinienanweisung mit enthält. `"Effect": "Allow"` `"Action": "Service:*"`

Beispielsweise führt die folgende Aussage in einer Richtlinie zu einem fehlgeschlagenen Ergebnis.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:*",
  "Resource": "*"
}
```

Das Steuerelement schlägt auch fehl, wenn Sie `"Effect": "Allow"` mit verwenden`"NotAction": "service:*"`. In diesem Fall bietet das `NotAction` Element Zugriff auf alle Aktionen in einem AWS-Service, mit Ausnahme der in angegebenen Aktionen`NotAction`.

Diese Kontrolle gilt nur für vom Kunden verwaltete IAM-Richtlinien. Sie gilt nicht für IAM-Richtlinien, die von verwaltet werden. AWS

Wenn Sie Berechtigungen zuweisen AWS-Services, ist es wichtig, dass Sie den Umfang der zulässigen IAM-Aktionen in Ihren IAM-Richtlinien angeben. Sie sollten IAM-Aktionen nur auf die Aktionen beschränken, die benötigt werden. Auf diese Weise können Sie Berechtigungen mit den geringsten Rechten bereitstellen. Zu freizügige Richtlinien können zu einer Eskalation von Rechten führen, wenn die Richtlinien einem IAM-Prinzipal zugeordnet sind, für den die Genehmigung möglicherweise nicht erforderlich ist.

In einigen Fällen möchten Sie möglicherweise IAM-Aktionen zulassen, die ein ähnliches Präfix haben, z. B. und. `DescribeFlowLogs` `DescribeAvailabilityZones` In diesen autorisierten Fällen können Sie dem allgemeinen Präfix einen Platzhalter mit einem Suffix hinzufügen. z. B. `ec2:Describe*`.

Dieses Steuerelement ist erfolgreich, wenn Sie eine IAM-Aktion mit einem Präfix und einem Platzhalter mit Suffix verwenden. Beispielsweise führt die folgende Anweisung in einer Richtlinie zu einem erfolgreichen Ergebnis.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:Describe*",
```

```
  "Resource": "*"
}
```

Wenn Sie verwandte IAM-Aktionen auf diese Weise gruppieren, können Sie auch verhindern, dass die Größenbeschränkungen der IAM-Richtlinie überschritten werden.

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Die globale Ressourcenaufzeichnung kann jedoch in einer einzigen Region aktiviert werden. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Um dieses Problem zu beheben, aktualisieren Sie Ihre IAM-Richtlinien, sodass sie keine vollen „*“ -Administratorrechte zulassen. Einzelheiten zur Bearbeitung einer IAM-Richtlinie finden Sie unter Bearbeiten von IAM-Richtlinien im IAM-Benutzerhandbuch.

[IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/1.12, CIS Foundations Benchmark v1.4.0/1.12 AWS

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::IAM::User`

AWS Config Regel: **`iam-user-unused-credentials-check`**

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob Ihre IAM-Benutzer über Passwörter oder aktive Zugriffsschlüssel verfügen, die 45 Tage oder länger nicht verwendet wurden. Zu diesem Zweck wird geprüft, ob der `maxCredentialUsageAge` Parameter der AWS Config Regel 45 oder mehr beträgt.

Benutzer können mit verschiedenen Arten von Anmeldeinformationen wie Kennwörtern oder Zugriffsschlüsseln auf AWS Ressourcen zugreifen.

CIS empfiehlt, alle Anmeldeinformationen zu entfernen oder zu deaktivieren, die 45 Tage oder länger nicht verwendet wurden. Durch das Deaktivieren oder Entfernen unnötiger Anmeldeinformationen reduzieren Sie den möglichen Schaden, der mit den Anmeldeinformationen eines kompromittierten oder ungenutzten Kontos angerichtet werden kann.

Die AWS Config Regel für dieses Steuerelement verwendet die Operationen `GetCredentialReport`und `GenerateCredentialReport`API, die nur alle vier Stunden aktualisiert werden. Es kann bis zu vier Stunden dauern, bis Änderungen an IAM-Benutzern für dieses Steuerelement sichtbar sind.

> **Note**
>
> AWS Config sollte in allen Regionen aktiviert sein, in denen Sie Security Hub verwenden. Sie können jedoch die Aufzeichnung globaler Ressourcen in einer einzigen Region aktivieren. Wenn Sie nur globale Ressourcen in einer einzelnen Region erfassen, können Sie diese Kontrolle in allen Regionen mit Ausnahme der Region deaktivieren, in der Sie globale Ressourcen aufzeichnen.

Abhilfe

Wenn Sie Benutzerinformationen in der IAM-Konsole anzeigen, gibt es Spalten für das Alter des Zugriffsschlüssels, das Alter des Kennworts und die letzte Aktivität. Wenn der Wert in einer dieser Spalten mehr als 45 Tage beträgt, deaktivieren Sie die Anmeldeinformationen für diese Benutzer.

Sie können auch Berichte über Anmeldeinformationen verwenden, um Benutzer zu überwachen und Benutzer zu identifizieren, die 45 oder mehr Tage lang keine Aktivität hatten. Sie können Berichte über Anmeldeinformationen im `.csv` Format von der IAM-Konsole herunterladen.

Nachdem Sie die inaktiven Konten oder ungenutzten Anmeldeinformationen identifiziert haben, deaktivieren Sie sie. Anweisungen finden Sie im IAM-Benutzerhandbuch unter Erstellen, Ändern oder Löschen eines IAM-Benutzerkennworts (Konsole).

[IAM.23] IAM Access Analyzer-Analyzer sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AccessAnalyzer::Analyzer`

AWS Config Regel: `tagged-accessanalyzer-analyzer` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein von AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) verwalteter Analyzer über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Analyzer keine Tagschlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Analyzer mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen

anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Analyzer finden Sie TagResourcein der AWS IAM Access Analyzer API-Referenz.

[IAM.24] IAM-Rollen sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IAM::Role`

AWS Config Regel: `tagged-iam-role` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList	Liste der Tags, die die AWS	`No default value`

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen	

Dieses Steuerelement prüft, ob eine AWS Identity and Access Management (IAM-) Rolle Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn die Rolle keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Rolle mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer IAM-Rolle finden Sie unter Tagging IAM-Ressourcen im IAM-Benutzerhandbuch.

[IAM.25] IAM-Benutzer sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IAM::User`

AWS Config Regel: `tagged-iam-user` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein AWS Identity and Access Management (IAM-) Benutzer über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Benutzer keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Benutzer mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem IAM-Benutzer finden Sie unter Tagging IAM-Ressourcen im IAM-Benutzerhandbuch.

[IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden

Verwandte Anforderungen: CIS Foundations Benchmark v3.0.0/1.19 AWS

Kategorie: Identifizieren > Konformität

Schweregrad: Mittel

Art der Ressource: `AWS::IAM::ServerCertificate`

AWS Config Regel: **`iam-server-certificate-expiration-check`**

Art des Zeitplans: Periodisch

Parameter: Keine

Mit dieser Steuerung wird geprüft, ob ein aktives SSL/TLS-Serverzertifikat, das in IAM verwaltet wird, abgelaufen ist. Die Kontrolle schlägt fehl, wenn das abgelaufene SSL/TLS-Serverzertifikat nicht entfernt wird.

Um HTTPS-Verbindungen zu Ihrer Website oder Anwendung zu aktivieren AWS, benötigen Sie ein SSL/TLS-Serverzertifikat. Sie können IAM oder AWS Certificate Manager (ACM) verwenden, um Serverzertifikate zu speichern und bereitzustellen. Verwenden Sie IAM nur dann als Zertifikatsmanager, wenn Sie HTTPS-Verbindungen in einer Umgebung unterstützen müssen AWS-Region , die von ACM nicht unterstützt wird. IAM bietet eine sichere Verschlüsselungsmethode für Ihre privaten Schlüssel und speichert die verschlüsselte Version in einem SSL-Zertifikatspeicher in IAM. IAM unterstützt die Bereitstellung von Serverzertifikaten in allen Regionen, Sie müssen Ihr Zertifikat jedoch von einem externen Anbieter beziehen, damit Sie es verwenden können. AWS Sie können kein ACM-Zertifikat auf IAM hochladen. Darüber hinaus können Sie Ihre Zertifikate nicht von der IAM-Konsole aus verwalten. Durch das Entfernen abgelaufener SSL/TLS-Zertifikate wird das Risiko vermieden, dass versehentlich ein ungültiges Zertifikat für eine Ressource bereitgestellt wird, wodurch die Glaubwürdigkeit der zugrunde liegenden Anwendung oder Website beeinträchtigt werden kann.

Abhilfe

Informationen zum Entfernen eines Serverzertifikats aus IAM finden Sie unter Verwalten von Serverzertifikaten in IAM im IAM-Benutzerhandbuch.

[IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess

Verwandte Anforderungen: CIS Foundations Benchmark v3.0.0/1.22 AWS

Kategorie: Schützen > Sichere Zugriffsverwaltung > Sichere IAM-Richtlinien

Schweregrad: Mittel

Ressourcentyp:`AWS::IAM::Role`,, `AWS::IAM::User` `AWS::IAM::Group`

AWS Config regel: **`iam-policy-blacklisted-check`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- „policyArns“: „arn:aws:iam: :aws:policy/, arn:aws-cn:iam: :aws:policy/, arn ::iam: :aws:policy/ AWSCloudShellFullAccess“ AWSCloudShellFullAccess aws-us-gov AWSCloudShellFullAccess

Dieses Steuerelement prüft, ob eine IAM-Identität (Benutzer, Rolle oder Gruppe) mit der verwalteten Richtlinie verknüpft ist. AWS `AWSCloudShellFullAccess` Die Steuerung schlägt fehl, wenn die `AWSCloudShellFullAccess` Richtlinie an eine IAM-Identität angehängt ist.

AWS CloudShell bietet eine bequeme Möglichkeit, CLI-Befehle auszuführen AWS-Services. Die AWS verwaltete Richtlinie `AWSCloudShellFullAccess` bietet vollen Zugriff CloudShell auf und ermöglicht somit das Hoch- und Herunterladen von Dateien zwischen dem lokalen System eines Benutzers und der CloudShell Umgebung. Innerhalb der CloudShell Umgebung verfügt ein Benutzer über Sudo-Berechtigungen und kann auf das Internet zugreifen. Das Anhängen dieser verwalteten Richtlinie an eine IAM-Identität gibt ihnen somit die Möglichkeit, Dateiübertragungssoftware zu installieren und Daten von externen Internetservern CloudShell zu verschieben. Wir empfehlen, dem Prinzip der geringsten Rechte zu folgen und Ihren IAM-Identitäten engere Berechtigungen zuzuweisen.

Abhilfe

Informationen zum Trennen der *`AWSCloudShellFullAccess`* Richtlinie von einer IAM-Identität finden Sie unter Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im IAM-Benutzerhandbuch.

[IAM.28] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein

Verwandte Anforderungen: CIS Foundations Benchmark v3.0.0/1.20 AWS

Kategorie: Erkennen > Erkennungsdienste > Überwachung privilegierter Nutzung

Schweregrad: Hoch

Art der Ressource: `AWS::AccessAnalyzer::Analzyer`

AWS Config Regel: **`iam-external-access-analyzer-enabled`**

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob AWS-Konto ein externer Zugriffsanalysator für IAM Access Analyzer aktiviert ist. Die Steuerung schlägt fehl, wenn für das Konto in Ihrem aktuell ausgewählten AWS-Region Konto kein External Access Analyzer aktiviert ist.

Die externen Zugriffsanalysatoren von IAM Access Analyzer helfen dabei, Ressourcen in Ihrer Organisation und Konten zu identifizieren, wie z. B. Amazon Simple Storage Service (Amazon S3) -Buckets oder IAM-Rollen, die mit einer externen Entität gemeinsam genutzt werden. Auf diese Weise können Sie einen unbeabsichtigten Zugriff auf Ihre Ressourcen und Daten vermeiden. IAM Access Analyzer ist regional und muss in jeder Region aktiviert sein. Um Ressourcen zu identifizieren, die gemeinsam mit externen Principals genutzt werden, analysiert ein Access Analyzer die ressourcenbasierten Richtlinien in Ihrer Umgebung anhand von logischen Argumenten. AWS Wenn Sie einen externen Zugriffsanalysator aktivieren, erstellen Sie einen Analyzer für Ihre gesamte Organisation oder Ihr Konto.

Abhilfe

Informationen zur Aktivierung eines External Access Analyzers in einer bestimmten Region finden Sie unter Enabling IAM Access Analyzer im IAM-Benutzerhandbuch. Sie müssen in jeder Region, in der Sie den Zugriff auf Ihre Ressourcen überwachen möchten, einen Analyzer aktivieren.

AWS IoT steuert

Diese Kontrollen beziehen sich auf AWS IoT Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::SecurityProfile`

AWS Config Regel: `tagged-iot-securityprofile` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein AWS IoT Core Sicherheitsprofil Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn das Sicherheitsprofil keine Tagschlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn das Sicherheitsprofil mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS IoT Core Sicherheitsprofil finden Sie unter Taggen Ihrer AWS IoT Ressourcen im AWS IoT Entwicklerhandbuch.

[IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::MitigationAction`

AWS Config Regel: `tagged-iot-mitigationaction` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob eine AWS IoT Core Minderungsaktion Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Schadensbegrenzungsaktion keine Tagschlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Abhilfemaßnahme mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS IoT Core Schadensbegrenzungsmaßnahme finden Sie unter Taggen Ihrer AWS IoT Ressourcen im Entwicklerhandbuch.AWS IoT

[IoT.3] AWS IoT Core -Dimensionen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::Dimension`

AWS Config Regel: `tagged-iot-dimension` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob eine AWS IoT Core Dimension über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn die Dimension keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Dimension mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS IoT Core Dimension finden Sie unter Taggen Ihrer AWS IoT Ressourcen im AWS IoT Entwicklerhandbuch.

[IoT.4] AWS IoT Core Autorisierer sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::Authorizer`

AWS Config Regel: `tagged-iot-authorizer` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList	Liste der Tags, die die AWS	`No default value`

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen	

Dieses Steuerelement prüft, ob ein AWS IoT Core Autorisierer über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn der Autorisierer keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Autorisierer mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS IoT Core Autorisierer finden Sie unter Taggen Ihrer AWS IoT Ressourcen im Entwicklerhandbuch.AWS IoT

[IoT.5] AWS IoT Core Rollenaliase sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::RoleAlias`

AWS Config Regel: `tagged-iot-rolealias` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein AWS IoT Core Rollenalias Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn der Rollenalias keine Tagschlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Rollenalias mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem AWS IoT Core Rollenalias finden Sie unter Taggen Ihrer AWS IoT Ressourcen im AWS IoT Entwicklerhandbuch.

[IoT.6] AWS IoT Core Richtlinien sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::IoT::Policy`

AWS Config Regel: `tagged-iot-policy` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob eine AWS IoT Core Richtlinie Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn die Richtlinie keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Richtlinie mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer AWS IoT Core Richtlinie finden Sie unter Taggen Ihrer AWS IoT Ressourcen im AWS IoT Entwicklerhandbuch.

Amazon Kinesis Kinesis-Steuerung

Diese Steuerungen beziehen sich auf Kinesis-Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::Kinesis::Stream`

AWS Config -Regel: `kinesis-stream-encrypted`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Kinesis Data Streams im Ruhezustand mit serverseitiger Verschlüsselung verschlüsselt sind. Diese Steuerung schlägt fehl, wenn ein Kinesis-Stream im Ruhezustand nicht mit serverseitiger Verschlüsselung verschlüsselt ist.

Serverseitige Verschlüsselung ist eine Funktion in Amazon Kinesis Data Streams, die Daten automatisch verschlüsselt, bevor sie sich im Ruhezustand befinden, mithilfe eines. AWS KMS key Die Daten werden verschlüsselt, bevor sie in die Speicherschicht des Kinesis-Streams geschrieben werden. Nach Abruf aus dem Speicher werden sie entschlüsselt. Daher werden Ihre Daten im Ruhezustand innerhalb des Amazon Kinesis Data Streams Streams-Service verschlüsselt.

Abhilfe

Informationen zur Aktivierung der serverseitigen Verschlüsselung für Kinesis-Streams finden Sie unter Wie fange ich mit serverseitiger Verschlüsselung an? im Amazon Kinesis Developer Guide.

[Kinesis.2] Kinesis-Streams sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Kinesis::Stream`

AWS Config Regel: `tagged-kinesis-stream` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon Kinesis Kinesis-Datenstream Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt

fehl, wenn der Datenstream keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Datenstrom mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Kinesis-Datenstream finden Sie unter Tagging your streams in Amazon Kinesis Data Streams im Amazon Kinesis Developer Guide.

AWS Key Management Service steuert

Diese Kontrollen beziehen sich auf AWS KMS Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen

Verwandte Anforderungen: NIST.800-53.R5 AC-2, NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-5, NIST.800-53.R5 AC-6, NIST.800-53.R5 R5 AC-6 (3)

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::IAM::Policy`

AWS Config -Regel: `iam-customer-policy-blocked-kms-actions`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`(nicht anpassbar)
- `excludePermissionBoundaryPolicy`: `True` (nicht anpassbar)

Überprüft, ob die Standardversion der vom Kunden verwalteten IAM-Richtlinien es Prinzipalen erlaubt, die AWS KMS Entschlüsselungsaktionen für alle Ressourcen zu verwenden. Die Steuerung schlägt fehl, wenn die Richtlinie offen genug ist, um `kms:ReEncryptFrom` Aktionen für alle `kms:Decrypt` KMS-Schlüssel zuzulassen.

Das Steuerelement überprüft nur KMS-Schlüssel im Resource-Element und berücksichtigt keine Bedingungen im Condition-Element einer Richtlinie. Darüber hinaus bewertet das Steuerelement sowohl angehängte als auch nicht verknüpfte, vom Kunden verwaltete Richtlinien. Inline-Richtlinien oder AWS verwaltete Richtlinien werden nicht geprüft.

Damit kontrollieren Sie AWS KMS, wer Ihre KMS-Schlüssel verwenden und auf Ihre verschlüsselten Daten zugreifen kann. IAM-Richtlinien definieren, welche Aktionen eine Identität (Benutzer, Gruppe oder Rolle) auf welchen Ressourcen ausführen kann. Gemäß den bewährten Sicherheitsmethoden wird AWS empfohlen, die geringsten Rechte zuzulassen. Mit anderen Worten, Sie sollten Identitäten nur die `kms:ReEncryptFrom` Berechtigungen `kms:Decrypt` oder und nur die Schlüssel gewähren, die zur Ausführung einer Aufgabe erforderlich sind. Andernfalls verwendet der Benutzer möglicherweise Schlüssel, die für Ihre Daten nicht geeignet sind.

Anstatt Berechtigungen für alle Schlüssel zu gewähren, sollten Sie die Mindestanzahl an Schlüsseln festlegen, die Benutzer für den Zugriff auf verschlüsselte Daten benötigen. Entwerfen Sie dann Richtlinien, die es Benutzern ermöglichen, nur diese Schlüssel zu verwenden. Erlauben Sie beispielsweise nicht die `kms:Decrypt` Erlaubnis für alle KMS-Schlüssel. Erlauben Sie stattdessen `kms:Decrypt` nur Schlüssel in einer bestimmten Region für Ihr Konto. Durch die Anwendung des Prinzips der geringsten Rechte können Sie das Risiko einer unbeabsichtigten Offenlegung Ihrer Daten verringern.

Abhilfe

Informationen zum Ändern einer vom Kunden verwalteten IAM-Richtlinie finden Sie unter Bearbeiten von kundenverwalteten Richtlinien im IAM-Benutzerhandbuch. Wenn Sie Ihre Richtlinie bearbeiten, geben Sie für das `Resource` Feld den Amazon-Ressourcennamen (ARN) des spezifischen Schlüssels oder der Schlüssel an, für die Sie Entschlüsselungsaktionen zulassen möchten.

[KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen

Verwandte Anforderungen: NIST.800-53.R5 AC-2, NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-5, NIST.800-53.R5 AC-6, NIST.800-53.R5 R5 AC-6 (3)

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource:

- `AWS::IAM::Group`
- `AWS::IAM::Role`
- `AWS::IAM::User`

AWS Config -Regel: `iam-inline-policy-blocked-kms-actions`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`(nicht anpassbar)

Dieses Steuerelement prüft, ob die in Ihre IAM-Identitäten (Rolle, Benutzer oder Gruppe) eingebetteten Inline-Richtlinien die AWS KMS Entschlüsselung und erneute Verschlüsselung aller KMS-Schlüssel zulassen. Die Steuerung schlägt fehl, wenn die Richtlinie offen genug ist, um `kms:ReEncryptFrom` Aktionen für alle `kms:Decrypt` KMS-Schlüssel zuzulassen.

Das Steuerelement überprüft nur KMS-Schlüssel im Resource-Element und berücksichtigt keine Bedingungen im Condition-Element einer Richtlinie.

Mit steuern Sie AWS KMS, wer Ihre KMS-Schlüssel verwenden und auf Ihre verschlüsselten Daten zugreifen kann. IAM-Richtlinien definieren, welche Aktionen eine Identität (Benutzer, Gruppe oder Rolle) auf welchen Ressourcen ausführen kann. Gemäß den bewährten Sicherheitsmethoden wird AWS empfohlen, die geringsten Rechte zuzulassen. Mit anderen Worten, Sie sollten Identitäten nur die Berechtigungen gewähren, die sie benötigen, und nur für Schlüssel, die zur Ausführung einer Aufgabe erforderlich sind. Andernfalls verwendet der Benutzer möglicherweise Schlüssel, die für Ihre Daten nicht geeignet sind.

Anstatt die Erlaubnis für alle Schlüssel zu erteilen, sollten Sie die Mindestanzahl an Schlüsseln festlegen, die Benutzer für den Zugriff auf verschlüsselte Daten benötigen. Entwerfen Sie dann Richtlinien, die es den Benutzern ermöglichen, nur diese Schlüssel zu verwenden. Erlauben Sie beispielsweise nicht die `kms:Decrypt` Erlaubnis für alle KMS-Schlüssel. Erlauben Sie die Erlaubnis stattdessen nur für bestimmte Schlüssel in einer bestimmten Region für Ihr Konto. Indem Sie das Prinzip der geringsten Rechte anwenden, können Sie das Risiko einer unbeabsichtigten Offenlegung Ihrer Daten verringern.

Abhilfe

Informationen zum Ändern einer IAM-Inline-Richtlinie finden Sie unter Bearbeiten von Inline-Richtlinien im IAM-Benutzerhandbuch. Wenn Sie Ihre Richtlinie bearbeiten, geben Sie für das `Resource` Feld den Amazon-Ressourcennamen (ARN) des spezifischen Schlüssels oder der Schlüssel an, für die Sie Entschlüsselungsaktionen zulassen möchten.

[KMS.3] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden

Verwandte Anforderungen: NIST.800-53.R5 SC-12, NIST.800-53.R5 SC-12 (2)

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Kritisch

Art der Ressource: `AWS::KMS::Key`

AWS Config Regel: `kms-cmk-not-scheduled-for-deletion-2` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Löschung von KMS-Schlüsseln geplant ist. Die Steuerung schlägt fehl, wenn das Löschen eines KMS-Schlüssels geplant ist.

KMS-Schlüssel können nach dem Löschen nicht wiederhergestellt werden. Mit einem KMS-Schlüssel verschlüsselte Daten können auch dauerhaft nicht wiederhergestellt werden, wenn der KMS-Schlüssel gelöscht wird. Wenn aussagekräftige Daten mit einem KMS-Schlüssel verschlüsselt wurden, der gelöscht werden soll, sollten Sie erwägen, die Daten zu entschlüsseln oder die Daten erneut mit einem neuen KMS-Schlüssel zu verschlüsseln, sofern Sie nicht absichtlich eine kryptografische Löschung durchführen.

Wenn das Löschen eines KMS-Schlüssels geplant ist, wird eine obligatorische Wartezeit durchgesetzt, damit genügend Zeit zur Verfügung steht, um den Löschvorgang rückgängig zu machen, falls er versehentlich geplant wurde. Die standardmäßige Wartezeit beträgt 30 Tage, kann aber auf bis zu 7 Tage reduziert werden, wenn der KMS-Schlüssel gelöscht werden soll. Während der Wartezeit kann das geplante Löschen abgebrochen werden und der KMS-Schlüssel wird nicht gelöscht.

Weitere Informationen zum Löschen von KMS-Schlüsseln finden Sie unter Löschen von KMS-Schlüsseln im AWS Key Management Service Entwicklerhandbuch.

Abhilfe

Informationen zum Abbrechen einer geplanten Löschung von KMS-Schlüsseln finden Sie im AWS Key Management Service Entwicklerhandbuch unter So brechen Sie das Löschen von Schlüsseln ab (Konsole) unter So brechen Sie das Löschen von Schlüsseln ab.

[KMS.4] Die AWS KMS Schlüsselrotation sollte aktiviert sein

Verwandte Anforderungen: PCI DSS v3.2.1/3.6.4, CIS AWS Foundations Benchmark v3.0.0/3.6, CIS Foundations Benchmark v1.4.0/3.8, CIS Foundations Benchmark v1.2.0/2.8, NIST.800-53.R5 SC-12, AWS NIST.800-53.R5 SC-12 (2), NIST.800-53.R5 AWS SC-28 (3)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-at-rest

Schweregrad: Mittel

Art der Ressource: `AWS::KMS::Key`

AWS Config -Regel: `cmk-backing-key-rotation-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

AWS KMS ermöglicht Kunden die Rotation des Backing-Schlüssels, bei dem es sich um Schlüsselmaterial handelt, das im KMS-Schlüssel gespeichert ist AWS KMS und mit der Schlüssel-ID des KMS-Schlüssels verknüpft ist. Der Unterstützungsschlüssel wird zum Durchführen kryptografischer Vorgänge wie z. B. Ver- und Entschlüsselungen verwendet. Die automatische Schlüsselrotation speichert derzeit alle vorherigen Unterstützungsschlüssel, sodass eine transparente Entschlüsselung verschlüsselter Daten erfolgen kann.

CIS empfiehlt, die KMS-Schlüsselrotation zu aktivieren. Das Rotieren der Verschlüsselungsschlüssel trägt zur Verringerung der potenziellen Auswirkungen eines kompromittierten Schlüssels bei, da der Zugriff auf mit einem neuen Schlüssel verschlüsselte Daten mit einem vorherigen Schlüssel, der möglicherweise kompromittiert wurde, nicht möglich ist.

Abhilfe

Informationen zur Aktivierung der KMS-Schlüsselrotation finden Sie unter So aktivieren und deaktivieren Sie die automatische Schlüsselrotation im AWS Key Management Service Entwicklerhandbuch.

AWS Lambda steuert

Diese Kontrollen beziehen sich auf Lambda-Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/7.2.1, NIST.800-53.R5 AC-21, NIST.800-53.r5 AC-3, NIst.800-53.r5 AC-3 (7), NIST.800-53.R5 AC-3 R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21)), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: `AWS::Lambda::Function`

AWS Config -Regel: `lambda-function-public-access-prohibited`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die ressourcenbasierte Richtlinie der Lambda-Funktion den öffentlichen Zugriff außerhalb Ihres Kontos verbietet. Die Kontrolle schlägt fehl, wenn der öffentliche Zugriff zulässig ist. Die Kontrolle schlägt auch fehl, wenn eine Lambda-Funktion von Amazon S3 aus aufgerufen wird und die Richtlinie keine Bedingung zur Beschränkung des öffentlichen Zugriffs enthält, wie z. `AWS:SourceAccount` Wir empfehlen, andere S3-Bedingungen zusammen mit `AWS:SourceAccount` in Ihrer Bucket-Richtlinie zu verwenden, um den Zugriff zu verfeinern.

Die Lambda-Funktion sollte nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihren Funktionscode ermöglichen kann.

Abhilfe

Um dieses Problem zu beheben, müssen Sie die ressourcenbasierte Richtlinie Ihrer Funktion aktualisieren, um Berechtigungen zu entfernen oder die Bedingung hinzuzufügen. `AWS:SourceAccount` Sie können die ressourcenbasierte Richtlinie nur über die Lambda-API oder aktualisieren. AWS CLI

Überprüfen Sie zunächst die ressourcenbasierte Richtlinie auf der Lambda-Konsole. Identifizieren Sie die Richtlinienaussage, deren `Principal` Feldwerte die Richtlinie öffentlich machen, z. B. oder. `"*"` `{ "AWS": "*" }`

Sie können die Richtlinie nicht von der Konsole aus bearbeiten. Um der Funktion Berechtigungen zu entziehen, führen Sie den `remove-permission`Befehl über den aus AWS CLI.

```
$ aws lambda remove-permission --function-name <function-name> --statement-
id <statement-id>
```

*`<function-name>`*Ersetzen Sie durch den Namen der Lambda-Funktion und *`<statement-id>`* durch die Anweisungs-ID (`Sid`) der Anweisung, die Sie entfernen möchten.

[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 SI-2, NIst.800-53.R5 SI-2 (2), NIst.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5)

Kategorie: Schutz > Sichere Entwicklung

Schweregrad: Mittel

Ressourcentyp: `AWS::Lambda::Function`

AWS Config -Regel: `lambda-function-settings-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `runtime`: `dotnet8, dotnet6, java21, java17, java11, java8.al2, nodejs20.x, nodejs18.x, nodejs16.x, python3.12, python3.11, python3.10, python3.9, python3.8, ruby3.3, ruby3.2` (nicht anpassbar)

Dieses Steuerelement prüft, ob die Laufzeiteinstellungen der AWS Lambda Funktionen mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Die Steuerung schlägt fehl, wenn die Lambda-Funktion keine unterstützte Laufzeit verwendet, wie bereits unter Parametern beschrieben. Security Hub ignoriert Funktionen mit dem Pakettyp`Image`.

Lambda-Laufzeiten basieren auf einer Kombination aus Betriebssystem, Programmiersprache und Softwarebibliotheken, die Wartungs- und Sicherheitsupdates unterliegen. Wenn eine Laufzeitkomponente für Sicherheitsupdates nicht mehr unterstützt wird, hat Lambda die Laufzeit als veraltet eingestuft. Auch wenn Sie keine Funktionen erstellen können, die die veraltete Runtime verwenden, ist die Funktion dennoch für die Verarbeitung von Aufrufereignissen verfügbar.
Wir empfehlen sicherzustellen, dass Ihre Lambda-Funktionen aktuell sind und keine veralteten Laufzeitumgebungen verwenden. Eine Liste der unterstützten Laufzeiten finden Sie unter Lambda-Laufzeiten im AWS Lambda Developer Guide.

Abhilfe

Weitere Informationen zu unterstützten Laufzeiten und Zeitplänen für veraltete Versionen finden Sie unter Runtime Deprecation Policy im Developer Guide.AWS Lambda Wenn Sie Ihre Laufzeiten auf die neueste Version migrieren, folgen Sie der Syntax und Anleitung der Herausgeber der Sprache.

Wir empfehlen außerdem, Runtime-Updates zu installieren, um das Risiko einer Beeinträchtigung Ihrer Workloads im seltenen Fall einer Runtime-Versionsinkompatibilität zu verringern.

[Lambda.3] Lambda-Funktionen sollten sich in einer VPC befinden

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, NIST.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 NIst.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Niedrig

Art der Ressource: `AWS::Lambda::Function`

AWS Config Regel: **`lambda-inside-vpc`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Lambda-Funktion in einer Virtual Private Cloud (VPC) bereitgestellt ist. Die Steuerung schlägt fehl, wenn die Lambda-Funktion nicht in einer VPC bereitgestellt wird. Security Hub bewertet die Konfiguration des VPC-Subnetz-Routings nicht, um die öffentliche Erreichbarkeit zu ermitteln. Möglicherweise werden fehlgeschlagene Ergebnisse für Lambda @Edge -Ressourcen angezeigt.

Die Bereitstellung von Ressourcen in einer VPC verbessert die Sicherheit und Kontrolle über Netzwerkkonfigurationen. Solche Bereitstellungen bieten auch Skalierbarkeit und hohe Fehlertoleranz über mehrere Availability Zones hinweg. Sie können VPC-Bereitstellungen an unterschiedliche Anwendungsanforderungen anpassen.

Abhilfe

Informationen zur Konfiguration einer vorhandenen Funktion zum Herstellen einer Verbindung zu privaten Subnetzen in Ihrer VPC finden Sie unter Konfiguration des VPC-Zugriffs im AWS Lambda Entwicklerhandbuch. Wir empfehlen, mindestens zwei private Subnetze für hohe Verfügbarkeit und mindestens eine Sicherheitsgruppe auszuwählen, die die Konnektivitätsanforderungen der Funktion erfüllt.

[Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren

Verwandte Anforderungen: NIst.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIst.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::Lambda::Function`

AWS Config -Regel: `lambda-vpc-multi-az-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`availabilityZones`	Mindestanzahl von Availability Zones	Enum	`2, 3, 4, 5, 6`	`2`

Dieses Steuerelement prüft, ob eine AWS Lambda Funktion, die eine Verbindung zu einer Virtual Private Cloud (VPC) herstellt, in mindestens der angegebenen Anzahl von Availability Zone (AZs) betrieben wird. Die Steuerung schlägt fehl, wenn die Funktion nicht in mindestens der angegebenen Anzahl von AZs funktioniert. Sofern Sie keinen benutzerdefinierten Parameterwert für die Mindestanzahl von AZs angeben, verwendet Security Hub einen Standardwert von zwei AZs.

Die Bereitstellung von Ressourcen auf mehreren AZs ist eine AWS bewährte Methode, um eine hohe Verfügbarkeit innerhalb Ihrer Architektur sicherzustellen. Verfügbarkeit ist eine zentrale Säule des dreifachen Sicherheitsmodells für Vertraulichkeit, Integrität und Verfügbarkeit. Alle Lambda-Funktionen, die eine Verbindung zu einer VPC herstellen, sollten über eine Multi-AZ-Bereitstellung verfügen, um sicherzustellen, dass eine einzelne Ausfallzone nicht zu einer vollständigen Betriebsunterbrechung führt.

Abhilfe

Wenn Sie Ihre Funktion so konfigurieren, dass sie eine Verbindung zu einer VPC in Ihrem Konto herstellt, geben Sie Subnetze in mehreren AZs an, um eine hohe Verfügbarkeit sicherzustellen. Anweisungen finden Sie unter Konfiguration des VPC-Zugriffs im AWS Lambda Entwicklerhandbuch.

Lambda führt automatisch andere Funktionen in mehreren AZs aus, um sicherzustellen, dass es für die Verarbeitung von Ereignissen im Falle einer Serviceunterbrechung in einer einzelnen Zone verfügbar ist.

[Lambda.6] Lambda-Funktionen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Lambda::Function`

AWS Config Regel: `tagged-lambda-function` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob eine AWS Lambda Funktion über Tags mit den spezifischen Tasten verfügt, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn

die Funktion keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Funktion mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Lambda-Funktion finden Sie unter Verwenden von Tags für Lambda-Funktionen im AWS Lambda Entwicklerhandbuch.

Amazon Macie-Steuerelemente

Diese Kontrollen beziehen sich auf Macie-Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Macie.1] Amazon Macie sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CA-7, NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 RA-5, NIST.800-53.R5 SA-8 (19), NIST.800-53.R5 SI-4

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `macie-status-check`

Art des Zeitplans: Periodisch

Diese Kontrolle prüft, ob Amazon Macie für ein Konto aktiviert ist. Die Kontrolle schlägt fehl, wenn Macie für das Konto nicht aktiviert ist.

Amazon Macie erkennt sensible Daten mithilfe von maschinellem Lernen und Musterabgleich, bietet Einblick in Datensicherheitsrisiken und ermöglicht automatisierten Schutz vor diesen Risiken. Macie bewertet Ihre Amazon Simple Storage Service (Amazon S3) -Buckets automatisch und kontinuierlich im Hinblick auf Sicherheit und Zugriffskontrolle und generiert Ergebnisse, um Sie über potenzielle Probleme mit der Sicherheit oder dem Datenschutz Ihrer Amazon S3-Daten zu informieren. Macie automatisiert auch die Erkennung und Meldung sensibler Daten, wie z. B. personenbezogener Daten (PII), um Ihnen ein besseres Verständnis der Daten zu vermitteln, die Sie in Amazon S3 speichern. Weitere Informationen finden Sie im Amazon Macie Macie-Benutzerhandbuch.

Abhilfe

Informationen zur Aktivierung von Macie finden Sie unter Macie aktivieren im Amazon Macie Macie-Benutzerhandbuch.

[Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CA-7, NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 RA-5, NIST.800-53.R5 SA-8 (19), NIST.800-53.R5 SI-4

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Hoch

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `macie-auto-sensitive-data-discovery-check`

Art des Zeitplans: Periodisch

Dieses Steuerelement prüft, ob die automatische Erkennung sensibler Daten für ein Amazon Macie-Administratorkonto aktiviert ist. Die Kontrolle schlägt fehl, wenn die automatische Erkennung sensibler Daten für ein Macie-Administratorkonto nicht aktiviert ist. Dieses Steuerelement gilt nur für Administratorkonten.

Macie automatisiert die Erkennung und Meldung sensibler Daten, wie z. B. persönlich identifizierbare Informationen (PII), in Amazon Simple Storage Service (Amazon S3) -Buckets. Mit der automatisierten Erkennung sensibler Daten bewertet Macie kontinuierlich Ihr Bucket-Inventar und verwendet Stichprobenverfahren, um repräsentative S3-Objekte aus Ihren Buckets zu identifizieren und auszuwählen. Macie analysiert dann die ausgewählten Objekte und untersucht sie auf sensible Daten. Im Verlauf der Analysen aktualisiert Macie Statistiken, Inventardaten und andere Informationen, die Macie zu Ihren S3-Daten bereitstellt. Macie generiert auch Ergebnisse, um gefundene sensible Daten zu melden.

Abhilfe

Informationen zum Erstellen und Konfigurieren automatisierter Discovery-Jobs für sensible Daten zur Analyse von Objekten in S3-Buckets finden Sie unter Konfiguration der automatisierten Erkennung sensibler Daten für Ihr Konto im Amazon Macie Macie-Benutzerhandbuch.

Amazon MSK-Steuerungen

Diese Kontrollen beziehen sich auf Ressourcen von Amazon Managed Streaming for Apache Kafka (Amazon MSK).

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden

Verwandte Anforderungen: NIst.800-53.R5 AC-4, NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-23, NIST.800-53.R5 SC-23 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIst.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 R5 SC-8 (2)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: `AWS::MSK::Cluster`

AWS Config -Regel: `msk-in-cluster-node-require-tls`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob ein Amazon MSK-Cluster bei der Übertragung mit HTTPS (TLS) zwischen den Broker-Knoten des Clusters verschlüsselt ist. Die Steuerung schlägt fehl, wenn die Klartext-Kommunikation für eine Cluster-Broker-Knotenverbindung aktiviert ist.

HTTPS bietet eine zusätzliche Sicherheitsebene, da TLS für die Übertragung von Daten verwendet wird, und kann dazu beitragen, potenzielle Angreifer daran zu hindern, person-in-the-middle Netzwerkverkehr mit oder ähnlichen Angriffen zu belauschen oder zu manipulieren. Standardmäßig verschlüsselt Amazon MSK Daten bei der Übertragung mit TLS. Sie können diese Standardeinstellung jedoch bei der Erstellung des Clusters überschreiben. Wir empfehlen die Verwendung verschlüsselter Verbindungen über HTTPS (TLS) für Broker-Knotenverbindungen.

Abhilfe

Informationen zum Aktualisieren der Verschlüsselungseinstellungen für MSK-Cluster finden Sie unter Aktualisieren der Sicherheitseinstellungen eines Clusters im Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein

Verwandte Anforderungen: NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-2

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Art der Ressource: `AWS::MSK::Cluster`

AWS Config -Regel: `msk-enhanced-monitoring-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen Amazon MSK-Cluster eine erweiterte Überwachung konfiguriert ist, die durch eine Überwachungsebene von mindestens `PER_TOPIC_PER_BROKER` angegeben wird. Die Steuerung schlägt fehl, wenn die Überwachungsebene für den Cluster auf `DEFAULT` oder `PER_BROKER` gesetzt ist.

Die `PER_TOPIC_PER_BROKER` Überwachungsebene bietet detailliertere Einblicke in die Leistung Ihres MSK-Clusters und bietet auch Metriken zur Ressourcennutzung, z. B. zur CPU- und Speicherauslastung. Auf diese Weise können Sie Leistungsengpässe und Ressourcennutzungsmuster für einzelne Themen und Broker identifizieren. Diese Transparenz kann wiederum die Leistung Ihrer Kafka-Broker optimieren.

Abhilfe

Gehen Sie wie folgt vor, um die erweiterte Überwachung für einen MSK-Cluster zu konfigurieren:

1. Öffnen Sie die Amazon-MSK-Konsole unter https://console.aws.amazon.com/msk/home?region=us-east-1#/home/.
2. Klicken Sie im Navigationsbereich auf Cluster. Wählen Sie dann einen Cluster aus.
3. Wählen Sie für Aktion die Option Überwachung bearbeiten aus.
4. Wählen Sie die Option für Erweiterte Überwachung auf Themenebene aus.
5. Wählen Sie Änderungen speichern aus.

Weitere Informationen zu Überwachungsebenen finden Sie unter Aktualisieren der Sicherheitseinstellungen eines Clusters im Amazon Managed Streaming for Apache Kafka Developer Guide.

Amazon MQ-Steuerelemente

Diese Kontrollen beziehen sich auf Amazon MQ MQ-Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch

Verwandte Anforderungen: NIST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-12, NIST.800-53.R5 SI-4

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::AmazonMQ::Broker`

AWS Config -Regel: `mq-cloudwatch-audit-log-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon MQ ActiveMQ-Broker Auditprotokolle an Amazon Logs streamt. CloudWatch Die Kontrolle schlägt fehl, wenn der Broker keine Auditprotokolle in Logs streamt. CloudWatch

Durch die Veröffentlichung von CloudWatch ActiveMQ-Broker-Protokollen in Logs können Sie CloudWatch Alarme und Metriken erstellen, die die Sichtbarkeit sicherheitsrelevanter Informationen erhöhen.

Abhilfe

Informationen zum Streamen von CloudWatch ActiveMQ-Broker-Protokollen in Logs finden Sie unter Konfiguration von Amazon MQ für ActiveMQ-Protokolle im Amazon MQ Developer Guide.

[MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CM-3, NIST.800-53.R5 SI-2

Kategorie: Identifizieren > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Niedrig

Art der Ressource: `AWS::AmazonMQ::Broker`

AWS Config -Regel: `mq-auto-minor-version-upgrade-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob bei einem Amazon MQ-Broker das automatische Upgrade für Nebenversionen aktiviert ist. Die Kontrolle schlägt fehl, wenn der Broker das automatische Upgrade der Nebenversion nicht aktiviert hat.

Da Amazon MQ neue Broker-Engine-Versionen veröffentlicht und unterstützt, sind die Änderungen abwärtskompatibel mit einer vorhandenen Anwendung und verwerfen keine bestehenden Funktionen. Automatische Versionsupdates der Broker Engine schützen Sie vor Sicherheitsrisiken, helfen bei der Behebung von Fehlern und verbessern die Funktionalität.

> **Note**
>
> Wenn der Broker, der mit dem automatischen Upgrade einer Nebenversion verknüpft ist, seinen neuesten Patch installiert hat und nicht mehr unterstützt wird, müssen Sie für das Upgrade manuelle Maßnahmen ergreifen.

Abhilfe

Informationen zum Aktivieren des automatischen Upgrades der Nebenversion für einen MQ-Broker finden Sie unter Automatisches Upgrade der Nebenversion der Engine im Amazon MQ Developer Guide.

[MQ.4] Amazon MQ-Broker sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::AmazonMQ::Broker`

AWS Config Regel: `tagged-amazonmq-broker` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList	Liste der Tags, die die AWS	`No default value`

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen	

Dieses Steuerelement prüft, ob ein Amazon MQ-Broker über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Broker keine Tag-Schlüssel hat oder wenn er nicht über alle im Parameter `requiredTagKeys` angegebenen Schlüssel verfügt. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Broker mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon MQ-Broker finden Sie unter Tagging resources im Amazon MQ Developer Guide.

[MQ.5] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Niedrig

Art der Ressource: `AWS::AmazonMQ::Broker`

AWS Config -Regel: `mq-active-deployment-mode`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Bereitstellungsmodus für einen Amazon MQ ActiveMQ-Broker auf Aktiv/Standby eingestellt ist. Die Steuerung schlägt fehl, wenn ein Single-Instance-Broker (standardmäßig aktiviert) als Bereitstellungsmodus festgelegt ist.

Die Aktiv-/Standby-Bereitstellung bietet Hochverfügbarkeit für Ihre Amazon MQ ActiveMQ-Broker in einem. AWS-Region Der Aktiv-/Standby-Bereitstellungsmodus umfasst zwei Broker-Instances in zwei verschiedenen Availability Zones, die in einem redundanten Paar konfiguriert sind. Diese Broker kommunizieren synchron mit Ihrer Anwendung, wodurch Ausfallzeiten und Datenverluste im Falle eines Fehlers reduziert werden können.

Abhilfe

Informationen zum Erstellen eines neuen ActiveMQ-Brokers mit aktivem Bereitstellungsmodus finden Sie unter Erstellen und Konfigurieren eines ActiveMQ-Brokers im Amazon MQ Developer Guide. Wählen Sie für den Bereitstellungsmodus die Option Active/Standby-Broker. Sie können den Bereitstellungsmodus für einen vorhandenen Broker nicht ändern. Stattdessen müssen Sie einen neuen Broker erstellen und die Einstellungen aus dem alten Broker kopieren.

[MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Niedrig

Art der Ressource: `AWS::AmazonMQ::Broker`

AWS Config -Regel: `mq-rabbit-deployment-mode`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Bereitstellungsmodus für einen Amazon MQ RabbitMQ-Broker auf Cluster-Bereitstellung eingestellt ist. Die Steuerung schlägt fehl, wenn ein Single-Instance-Broker (standardmäßig aktiviert) als Bereitstellungsmodus festgelegt ist.

Die Cluster-Bereitstellung bietet Hochverfügbarkeit für Ihre Amazon MQ RabbitMQ-Broker in einem. AWS-Region Die Cluster-Bereitstellung ist eine logische Gruppierung von drei RabbitMQ-Broker-Knoten, von denen jeder über ein eigenes Amazon Elastic Block Store (Amazon EBS) -Volume und einen gemeinsamen Status verfügt. Die Cluster-Bereitstellung stellt sicher, dass Daten auf alle Knoten im Cluster repliziert werden, wodurch Ausfallzeiten und Datenverluste im Falle eines Fehlers reduziert werden können.

Abhilfe

Informationen zum Erstellen eines neuen RabbitMQ-Brokers mit Cluster-Bereitstellungsmodus finden Sie unter Erstellen und Herstellen einer Verbindung zu einem RabbitMQ-Broker im Amazon MQ Developer Guide. Wählen Sie für den Bereitstellungsmodus die Option Cluster-Bereitstellung. Sie können den Bereitstellungsmodus für einen vorhandenen Broker nicht ändern. Stattdessen müssen Sie einen neuen Broker erstellen und die Einstellungen aus dem alten Broker kopieren.

Amazon Neptune Neptune-Steuerungen

Diese Kontrollen beziehen sich auf Neptunressourcen.

Diese Steuerungen sind möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `neptune-cluster-encrypted`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Neptune-DB-Cluster im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn ein Neptune-DB-Cluster im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf alle Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch Verschlüsselung können Sie die Vertraulichkeit solcher Daten schützen und so das Risiko verringern, dass ein unberechtigter Benutzer darauf zugreifen kann. Die Verschlüsselung Ihrer Neptune-DB-Cluster schützt Ihre Daten und Metadaten vor unbefugtem Zugriff. Es erfüllt auch die Compliance-Anforderungen für die data-at-rest Verschlüsselung von Produktionsdateisystemen.

Abhilfe

Sie können die Verschlüsselung im Ruhezustand aktivieren, wenn Sie einen Neptune-DB-Cluster erstellen. Sie können die Verschlüsselungseinstellungen nach dem Erstellen eines Clusters nicht ändern. Weitere Informationen finden Sie unter Encrypting Neptune resources at rest im Neptune-Benutzerhandbuch.

[Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.r5

AU-3 R5 AU-6 (1), NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 AU-6 (5), NIST.800-53.R5 AU-7 (1), NIST.800-53.R5 AU-9 (7), NIST.800-53.r5 CA-7, NIST.800-53.R5 CA-7, NIST.800-53.R5 R5 SC-7 (9), NIST.800-53.R5 SI-20, NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-4 (5), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `neptune-cluster-cloudwatch-log-export-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob ein Neptune-DB-Cluster Audit-Logs in Amazon CloudWatch Logs veröffentlicht. Die Steuerung schlägt fehl, wenn ein Neptune-DB-Cluster keine Audit-Logs in Logs veröffentlicht. CloudWatch `EnableCloudWatchLogsExport`sollte auf eingestellt sein. `Audit`

Amazon Neptune und Amazon CloudWatch sind integriert, sodass Sie Leistungskennzahlen sammeln und analysieren können. Neptune sendet automatisch Messwerte an Alarme CloudWatch und unterstützt CloudWatch diese auch. Audit-Logs sind hochgradig anpassbar. Wenn Sie eine Datenbank prüfen, kann jeder Vorgang an den Daten überwacht und in einem Audit-Trail protokolliert werden, einschließlich Informationen darüber, auf welchen Datenbankcluster zugegriffen wird und wie. Wir empfehlen, diese Protokolle an zu senden, CloudWatch um Ihnen bei der Überwachung Ihrer Neptune-DB-Cluster zu helfen.

Abhilfe

Informationen zum Veröffentlichen von Neptune-Audit-Logs in CloudWatch Logs finden Sie unter Neptune-Logs in Amazon CloudWatch Logs veröffentlichen im Neptune-Benutzerhandbuch. Wählen Sie im Abschnitt Protokollexporte die Option Audit aus.

[Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein

Verwandte Anforderungen: NIST.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20),

NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Kritisch

Art der Ressource: `AWS::RDS::DBClusterSnapshot`

AWS Config -Regel: `neptune-cluster-snapshot-public-prohibited`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein manueller Neptune-DB-Cluster-Snapshot öffentlich ist. Die Steuerung schlägt fehl, wenn ein manueller Neptune-DB-Cluster-Snapshot öffentlich ist.

Ein manueller Snapshot eines Neptune-DB-Clusters sollte nicht öffentlich sein, es sei denn, dies ist beabsichtigt. Wenn Sie einen unverschlüsselten manuellen Snapshot als öffentlich freigeben, ist der Snapshot für alle verfügbar. AWS-KontenÖffentliche Schnappschüsse können zu einer unbeabsichtigten Offenlegung von Daten führen.

Abhilfe

Informationen zum Entfernen des öffentlichen Zugriffs für manuelle Neptune-DB-Cluster-Snapshots finden Sie unter Freigeben eines DB-Cluster-Snapshots im Neptune-Benutzerhandbuch.

[Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2), NIST.800-53.R5 CM-3, NIST.800-53.R5 SC-5 (2)

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `neptune-cluster-deletion-protection-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem Neptune-DB-Cluster der Löschschutz aktiviert ist. Die Steuerung schlägt fehl, wenn für einen Neptune-DB-Cluster kein Löschschutz aktiviert ist.

Die Aktivierung des Cluster-Löschschutzes bietet eine zusätzliche Schutzebene vor dem versehentlichen Löschen von Datenbanken oder vor dem Löschen durch einen nicht autorisierten Benutzer. Ein Neptune-DB-Cluster kann nicht gelöscht werden, solange der Löschschutz aktiviert ist. Sie müssen zuerst den Löschschutz deaktivieren, bevor eine Löschanfrage erfolgreich sein kann.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für einen vorhandenen Neptune-DB-Cluster finden Sie unter Ändern des DB-Clusters mithilfe der Konsole, der CLI und der API im Amazon Aurora Aurora-Benutzerhandbuch.

[Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 SI-12

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: `AWS::RDS::DBCluster`

AWS Config -Regel: `neptune-cluster-backup-retention-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert	
`minimumBackupReten`	Minimale Aufbewahrungsdauer für Backups in Tagen	Ganzzahl	7 auf 35	7	

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert	
`tionPeriod`					

Dieses Steuerelement prüft, ob in einem Neptune-DB-Cluster automatische Backups aktiviert sind und ob die Aufbewahrungsfrist für Backups größer oder gleich dem angegebenen Zeitraum ist. Die Kontrolle schlägt fehl, wenn Backups für den Neptune-DB-Cluster nicht aktiviert sind oder wenn die Aufbewahrungszeit kürzer als der angegebene Zeitrahmen ist. Sofern Sie keinen benutzerdefinierten Parameterwert für die Aufbewahrungsdauer von Backups angeben, verwendet Security Hub einen Standardwert von 7 Tagen.

Backups helfen Ihnen, sich nach einem Sicherheitsvorfall schneller zu erholen und die Widerstandsfähigkeit Ihrer Systeme zu stärken. Durch die Automatisierung von Backups für Ihre Neptune-DB-Cluster können Sie Ihre Systeme bis zu einem bestimmten Zeitpunkt wiederherstellen und Ausfallzeiten und Datenverluste minimieren.

Abhilfe

Informationen zur Aktivierung automatisierter Backups und zur Festlegung einer Aufbewahrungsfrist für Backups für Ihre Neptune-DB-Cluster finden Sie unter Automatisierte Backups aktivieren im Amazon RDS-Benutzerhandbuch. Wählen Sie für den Aufbewahrungszeitraum für Backup einen Wert größer oder gleich 7.

[Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SC-7 (18)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBClusterSnapshot`

AWS Config -Regel: `neptune-cluster-snapshot-encrypted`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Neptune-DB-Cluster-Snapshot im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn ein Neptune-DB-Cluster im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf alle Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch Verschlüsselung können Sie die Vertraulichkeit solcher Daten schützen und so das Risiko verringern, dass ein nicht autorisierter Benutzer darauf zugreifen kann. Daten in Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden, um eine zusätzliche Sicherheitsebene zu gewährleisten.

Abhilfe

Sie können einen vorhandenen Neptune-DB-Cluster-Snapshot nicht verschlüsseln. Stattdessen müssen Sie den Snapshot in einem neuen DB-Cluster wiederherstellen und die Verschlüsselung auf dem Cluster aktivieren. Sie können einen verschlüsselten Snapshot aus dem verschlüsselten Cluster erstellen. Anweisungen finden Sie unter Wiederherstellung aus einem DB-Cluster-Snapshot und Erstellen eines DB-Cluster-Snapshots in Neptune im Neptune-Benutzerhandbuch.

[Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.r5 AC-6

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `neptune-cluster-iam-database-authentication`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem Neptune-DB-Cluster die IAM-Datenbankauthentifizierung aktiviert ist. Die Steuerung schlägt fehl, wenn die IAM-Datenbankauthentifizierung für einen Neptune-DB-Cluster nicht aktiviert ist.

Die IAM-Datenbankauthentifizierung für Amazon Neptune Neptune-Datenbankcluster macht das Speichern von Benutzeranmeldeinformationen in der Datenbankkonfiguration überflüssig, da die Authentifizierung extern mithilfe von IAM verwaltet wird. Wenn die IAM-Datenbankauthentifizierung aktiviert ist, muss jede Anfrage mit Signature Version 4 signiert werden. AWS

Abhilfe

Standardmäßig ist die IAM-Datenbankauthentifizierung deaktiviert, wenn Sie einen Neptune-DB-Cluster erstellen. Informationen zur Aktivierung finden Sie unter Aktivieren der IAM-Datenbankauthentifizierung in Neptune im Neptune-Benutzerhandbuch.

[Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2)

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `neptune-cluster-copy-tags-to-snapshot-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Neptune-DB-Cluster so konfiguriert ist, dass er alle Tags in Snapshots kopiert, wenn die Snapshots erstellt werden. Die Steuerung schlägt fehl, wenn ein Neptune-DB-Cluster nicht so konfiguriert ist, dass er Tags in Snapshots kopiert.

Die Identifizierung und Inventarisierung Ihrer IT-Ressourcen ist ein entscheidender Aspekt der Unternehmensführung und Sicherheit. Sie sollten Snapshots auf die gleiche Weise kennzeichnen wie ihre übergeordneten Amazon RDS-Datenbankcluster. Durch das Kopieren von Tags wird sichergestellt, dass die Metadaten für die DB-Snapshots mit denen der übergeordneten

Datenbankcluster übereinstimmen und dass die Zugriffsrichtlinien für den DB-Snapshot auch mit denen der übergeordneten DB-Instance übereinstimmen.

Abhilfe

Informationen zum Kopieren von Tags in Snapshots für Neptune-DB-Cluster finden Sie unter Kopieren von Tags in Neptune im Neptune-Benutzerhandbuch.

[Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `neptune-cluster-multi-az-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon Neptune Neptune-DB-Cluster über Read-Replica-Instances in mehreren Availability Zones (AZs) verfügt. Die Steuerung schlägt fehl, wenn der Cluster nur in einer AZ bereitgestellt wird.

Wenn eine AZ nicht verfügbar ist und während regelmäßiger Wartungsereignisse, dienen Read-Replicas als Failover-Ziele für die primäre Instanz. Wenn die primäre Instance ausfällt, stuft Neptune eine Read-Replica-Instance zur primären Instance herauf. Wenn Ihr DB-Cluster keine Read-Replica-Instances enthält, ist Ihr DB-Cluster bei einem Ausfall der primären Instance solange nicht verfügbar, bis sie neu erstellt wurde. Die Neuerstellung der primären Instance dauert erheblich länger als die Heraufstufung einer Read-Replica-Instance. Um eine hohe Verfügbarkeit zu gewährleisten, empfehlen wir, eine oder mehrere Read-Replica-Instances zu erstellen, die dieselbe DB-Instance-Klasse wie die primäre Instance haben und sich in anderen AZs als die primäre Instance befinden.

Abhilfe

Informationen zur Bereitstellung eines Neptune-DB-Clusters in mehreren AZs finden Sie unter Read-Replica-DB-Instances in einem Neptune-DB-Cluster im Neptune-Benutzerhandbuch.

AWS Network Firewall steuert

Diese Steuerungen beziehen sich auf die Ressourcen der Network Firewall.

Diese Steuerungen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::Firewall`

AWS Config -Regel: `netfw-multi-az-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement bewertet, ob eine über mehrere Availability Zones (AZs) verwaltete Firewall eingesetzt AWS Network Firewall wird. Die Steuerung schlägt fehl, wenn eine Firewall nur in einer AZ bereitgestellt wird.

AWS Die globale Infrastruktur umfasst mehrere AWS-Regionen. AZs sind physisch getrennte, isolierte Standorte innerhalb jeder Region, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Durch die Bereitstellung einer Netzwerk-Firewall-Firewall auf mehreren AZs können Sie den Verkehr zwischen AZs verteilen und verlagern, was Ihnen bei der Entwicklung hochverfügbarer Lösungen hilft.

Abhilfe

Bereitstellung einer Netzwerk-Firewall-Firewall auf mehreren AZs

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.

2. Wählen Sie im Navigationsbereich unter Network Firewall die Option Firewalls aus.
3. Wählen Sie auf der Seite Firewalls die Firewall aus, die Sie bearbeiten möchten.
4. Wählen Sie auf der Seite mit den Firewall-Details die Registerkarte Firewall-Details aus.
5. Wählen Sie im Abschnitt Zugeordnete Richtlinie und VPC die Option Bearbeiten aus.
6. Um eine neue AZ hinzuzufügen, wählen Sie Neues Subnetz hinzufügen. Wählen Sie die AZ und das Subnetz aus, die Sie verwenden möchten. Stellen Sie sicher, dass Sie mindestens zwei AZs auswählen.
7. Wählen Sie Speichern.

[NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (12), NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIst.800-53.R5 AU-10, NIst.800-53.R5 AU-2, NIST.800-53.R5 AU-2 800-53.R5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 AU-9 (7), NIST.800-53.R5 CA-7, NIst.800-53.R5 SC-7 (9), NIst.800-53.R5 SI-3 (8), NIst.800-53.R5 SI-4, NIST.800-53,R5 SI-4 (20), NIST.800-53,R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::LoggingConfiguration`

AWS Config -Regel: `netfw-logging-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung für eine AWS Network Firewall Firewall aktiviert ist. Die Steuerung schlägt fehl, wenn die Protokollierung für mindestens einen Protokolltyp nicht aktiviert ist oder wenn das Protokollierungsziel nicht existiert.

Mithilfe der Protokollierung können Sie die Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer Firewalls aufrechterhalten. In der Network Firewall bietet Ihnen die Protokollierung detaillierte Informationen über den Netzwerkverkehr, einschließlich der Uhrzeit, zu der die Stateful-Engine einen Paketfluss empfangen hat, detaillierte Informationen über den Paketfluss und alle statusbehafteten Regelaktionen, die gegen den Paketfluss ergriffen wurden.

Abhilfe

Informationen zum Aktivieren der Protokollierung für eine Firewall finden Sie unter Aktualisieren der Protokollierungskonfiguration einer Firewall im AWS Network Firewall Entwicklerhandbuch.

[NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schützen > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config -Regel: `netfw-policy-rule-group-associated`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob einer Netzwerk-Firewall-Richtlinie statusbehaftete oder statuslose Regelgruppen zugeordnet sind. Die Steuerung schlägt fehl, wenn keine statusfreien oder statusbehafteten Regelgruppen zugewiesen werden.

Eine Firewall-Richtlinie definiert, wie Ihre Firewall den Verkehr in Amazon Virtual Private Cloud (Amazon VPC) überwacht und verarbeitet. Die Konfiguration von statusfreien und statusbehafteten Regelgruppen hilft beim Filtern von Paketen und Datenströmen und definiert die standardmäßige Verarbeitung des Datenverkehrs.

Abhilfe

Informationen zum Hinzufügen einer Regelgruppe zu einer Netzwerk-Firewall-Richtlinie finden Sie unter Aktualisieren einer Firewall-Richtlinie im AWS Network Firewall Entwicklerhandbuch. Informationen zum Erstellen und Verwalten von Regelgruppen finden Sie unter Regelgruppen in AWS Network Firewall.

[NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schützen > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config -Regel: `netfw-policy-default-action-full-packets`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `statelessDefaultActions: aws:drop,aws:forward_to_sfe`(nicht anpassbar)

Dieses Steuerelement überprüft, ob die standardmäßige statuslose Aktion für vollständige Pakete für eine Netzwerkfirewall-Richtlinie Drop oder Forward ist. Die Steuerung ist erfolgreich, wenn `Drop` oder ausgewählt `Forward` ist, und schlägt fehl, wenn sie ausgewählt `Pass` ist.

Eine Firewall-Richtlinie definiert, wie Ihre Firewall den Verkehr in Amazon VPC überwacht und verarbeitet. Sie konfigurieren statusfreie und statusbehaftete Regelgruppen, um Pakete und Datenverkehrsströme zu filtern. Die Standardeinstellung `Pass` kann unbeabsichtigten Datenverkehr zulassen.

Abhilfe

Informationen zum Ändern Ihrer Firewall-Richtlinie finden Sie unter Aktualisieren einer Firewall-Richtlinie im AWS Network Firewall Entwicklerhandbuch. Wählen Sie für Standardaktionen ohne Status die Option Bearbeiten aus. Wählen Sie dann „Löschen“ oder „An statusbehaftete Regelgruppen weiterleiten“ als Aktion aus.

[NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schützen > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config -Regel: `netfw-policy-default-action-fragment-packets`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe`(nicht anpassbar)

Dieses Steuerelement prüft, ob die standardmäßige statuslose Aktion für fragmentierte Pakete für eine Netzwerk-Firewall-Richtlinie Drop oder Forward ist. Die Steuerung ist erfolgreich, wenn `Drop` oder ausgewählt `Forward` ist, und schlägt fehl, wenn sie ausgewählt `Pass` ist.

Eine Firewall-Richtlinie definiert, wie Ihre Firewall den Verkehr in Amazon VPC überwacht und verarbeitet. Sie konfigurieren statusfreie und statusbehaftete Regelgruppen, um Pakete und Datenverkehrsströme zu filtern. Die Standardeinstellung `Pass` kann unbeabsichtigten Datenverkehr zulassen.

Abhilfe

Informationen zum Ändern Ihrer Firewall-Richtlinie finden Sie unter Aktualisieren einer Firewall-Richtlinie im AWS Network Firewall Entwicklerhandbuch. Wählen Sie für Standardaktionen ohne Status die Option Bearbeiten aus. Wählen Sie dann „Löschen“ oder „An statusbehaftete Regelgruppen weiterleiten“ als Aktion aus.

[NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein

Verwandte Anforderungen: NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (5)

Kategorie: Schützen > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::RuleGroup`

AWS Config -Regel: `netfw-stateless-rule-group-not-empty`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine statuslose Regelgruppe Regeln AWS Network Firewall enthält. Das Steuerelement schlägt fehl, wenn die Regelgruppe keine Regeln enthält.

Eine Regelgruppe enthält Regeln, die definieren, wie Ihre Firewall den Verkehr in Ihrer VPC verarbeitet. Eine leere statuslose Regelgruppe kann, wenn sie in einer Firewallrichtlinie vorhanden ist, den Eindruck erwecken, dass die Regelgruppe den Datenverkehr verarbeitet. Wenn die statuslose Regelgruppe jedoch leer ist, verarbeitet sie keinen Datenverkehr.

Abhilfe

Informationen zum Hinzufügen von Regeln zu Ihrer Netzwerk-Firewall-Regelgruppe finden Sie unter Aktualisieren einer statusbehafteten Regelgruppe im AWS Network Firewall Entwicklerhandbuch. Wählen Sie auf der Seite mit den Firewall-Details für Stateless Rule Group die Option Bearbeiten aus, um Regeln hinzuzufügen.

[NetworkFirewall.7] Netzwerk-Firewall-Firewalls sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::NetworkFirewall::Firewall`

AWS Config Regel: `tagged-networkfirewall-firewall` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob eine AWS Network Firewall Firewall über Tags mit den spezifischen Schlüsseln verfügt, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn die Firewall keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Firewall mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Netzwerk-Firewall-Firewall finden Sie unter Tagging AWS Network Firewall resources im AWS Network Firewall Developer Guide.

[NetworkFirewall.8] Firewall-Richtlinien für Netzwerk-Firewalls sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config Regel: `tagged-networkfirewall-firewallpolicy` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob eine AWS Network Firewall Firewall-Richtlinie Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn die Firewall-Richtlinie keine Tagschlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Firewall-Richtlinie mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Netzwerk-Firewall-Richtlinie finden Sie unter Tagging AWS Network Firewall resources im AWS Network Firewall Developer Guide.

[NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2), NIST.800-53.R5 CM-3, NIST.800-53.R5 SC-5 (2)

Kategorie: Schützen > Netzwerksicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::NetworkFirewall::Firewall`

AWS Config -Regel: `netfw-deletion-protection-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine AWS Network Firewall Firewall der Löschschutz aktiviert ist. Die Steuerung schlägt fehl, wenn der Löschschutz für eine Firewall nicht aktiviert ist.

AWS Network Firewall ist ein zustandsorientierter, verwalteter Dienst für Netzwerk-Firewall und Erkennung von Eindringlingen, mit dem Sie den Datenverkehr zu, von oder zwischen Ihren Virtual

Private Clouds (VPCs) überprüfen und filtern können. Die Löschschutzeinstellung schützt vor versehentlichem Löschen der Firewall.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für eine bestehende Netzwerk-Firewall-Firewall finden Sie unter Aktualisieren einer Firewall im AWS Network Firewall Entwicklerhandbuch. Wählen Sie unter Änderungsschutz die Option Aktivieren aus. Sie können den Löschschutz auch aktivieren, indem Sie die UpdateFirewallDeleteProtectionAPI aufrufen und das `DeleteProtection` Feld auf setzen. `true`

Amazon OpenSearch Service-Kontrollen

Diese Kontrollen beziehen sich auf OpenSearch Serviceressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/7.2.1, NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.r5 SC-28, Nist.800-53.r5 SC-28, Nist.800-53.r5 NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-encrypted-at-rest`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für OpenSearch Domänen die encryption-at-rest Konfiguration aktiviert ist. Die Prüfung schlägt fehl, wenn die Verschlüsselung im Ruhezustand nicht aktiviert ist.

Für eine zusätzliche Sicherheitsebene für vertrauliche Daten sollten Sie Ihre OpenSearch Service-Domain so konfigurieren, dass sie im Ruhezustand verschlüsselt wird. Wenn Sie die Verschlüsselung von Daten im Ruhezustand konfigurieren, AWS KMS werden Ihre Verschlüsselungsschlüssel gespeichert und verwaltet. Für die Verschlüsselung wird der Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256) AWS KMS verwendet.

Weitere Informationen zur OpenSearch Service-Verschlüsselung im Ruhezustand finden Sie unter Verschlüsselung ruhender Daten für Amazon OpenSearch Service im Amazon OpenSearch Service Developer Guide.

Abhilfe

Informationen zur Aktivierung der Verschlüsselung im Ruhezustand für neue und bestehende OpenSearch Domains finden Sie unter Enabling encryption of data at rest im Amazon OpenSearch Service Developer Guide.

[Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.R5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.R5 AC-3. R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21)), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Kritisch

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-in-vpc-only`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob sich OpenSearch Domänen in einer VPC befinden. Es bewertet nicht die Konfiguration des VPC-Subnetz-Routings, um den öffentlichen Zugriff zu bestimmen.

Sie sollten sicherstellen, dass OpenSearch Domänen nicht an öffentliche Subnetze angehängt sind. Informationen zu ressourcenbasierten Richtlinien finden Sie im Amazon OpenSearch Service

Developer Guide. Sie sollten auch sicherstellen, dass Ihre VPC gemäß den empfohlenen bewährten Methoden konfiguriert ist. Bewährte Sicherheitsmethoden für Ihre VPC finden Sie im Amazon VPC-Benutzerhandbuch.

OpenSearch Domänen, die in einer VPC bereitgestellt werden, können über das private AWS Netzwerk mit VPC-Ressourcen kommunizieren, ohne das öffentliche Internet durchqueren zu müssen. Diese Konfiguration erhöht das Sicherheitsniveau, indem der Zugriff auf die Daten während der Übertragung eingeschränkt wird. VPCs bieten eine Reihe von Netzwerksteuerungen, um den Zugriff auf OpenSearch Domänen zu sichern, einschließlich Netzwerk-ACL und Sicherheitsgruppen. Security Hub empfiehlt, öffentliche OpenSearch Domains zu VPCs zu migrieren, um diese Kontrollen nutzen zu können.

Abhilfe

Wenn Sie eine Domäne mit einem öffentlichen Endpunkt erstellen, können Sie sie später nicht in einer VPC platzieren. Sie müssen stattdessen eine neue Domäne erstellen und die Daten übernehmen. Umgekehrt gilt dies auch. Wenn Sie eine Domäne innerhalb einer VPC erstellen, kann sie keinen öffentlichen Endpunkt haben. Stattdessen müssen Sie entweder eine andere Domäne erstellen oder dieses Steuerelement deaktivieren.

Anweisungen finden Sie unter Starten Ihrer Amazon OpenSearch Service-Domains innerhalb einer VPC im Amazon OpenSearch Service Developer Guide.

[Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

Verwandte Anforderungen: NIst.800-53.R5 AC-4, NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-23, NIST.800-53.R5 SC-23 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIst.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 R5 SC-8 (2)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten währen der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-node-to-node-encryption-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für OpenSearch Domänen die node-to-node Verschlüsselung aktiviert ist. Diese Kontrolle schlägt fehl, wenn die node-to-node Verschlüsselung in der Domain deaktiviert ist.

HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer den Netzwerkverkehr mit person-in-the-middle oder ähnlichen Angriffen abhören oder manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Durch die Aktivierung der node-to-node Verschlüsselung für OpenSearch Domänen wird sichergestellt, dass die Kommunikation innerhalb des Clusters während der Übertragung verschlüsselt wird.

Mit dieser Konfiguration kann es zu Leistungseinbußen kommen. Sie sollten sich der Leistungseinbußen bewusst sein und diese testen, bevor Sie diese Option aktivieren.

Abhilfe

Informationen zum Aktivieren der node-to-node Verschlüsselung für eine OpenSearch Domain finden Sie unter node-to-node Enabling encryption im Amazon OpenSearch Service Developer Guide.

Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.r5 AU-3 R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-logs-to-cloudwatch`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `logtype = 'error'`(nicht anpassbar)

Dieses Steuerelement prüft, ob OpenSearch Domänen so konfiguriert sind, dass sie CloudWatch Fehlerprotokolle an Logs senden. Dieses Steuerelement schlägt fehl, wenn die Fehlerprotokollierung für eine Domäne nicht aktiviert CloudWatch ist.

Sie sollten Fehlerprotokolle für OpenSearch Domänen aktivieren und diese CloudWatch Protokolle zur Aufbewahrung und Bearbeitung an Logs senden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Abhilfe

Informationen zum Aktivieren der Protokollveröffentlichung finden Sie unter Aktivieren der Protokollveröffentlichung (Konsole) im Amazon OpenSearch Service Developer Guide.

Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.r5 AU-3 R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-audit-logging-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `cloudWatchLogsLogGroupArnList`(nicht anpassbar) — Security Hub füllt diesen Parameter nicht aus. Durch Kommas getrennte Liste von CloudWatch Logs-Log-Gruppen, die für Audit-Logs konfiguriert werden sollten.

Diese Regel gilt, `NON_COMPLIANT` wenn die CloudWatch Logs-Protokollgruppe der OpenSearch Domäne nicht in dieser Parameterliste angegeben ist.

Dieses Steuerelement prüft, ob für OpenSearch Domänen die Auditprotokollierung aktiviert ist. Dieses Steuerelement schlägt fehl, wenn für eine OpenSearch Domäne die Überwachungsprotokollierung nicht aktiviert ist.

Audit-Logs sind in hohem Maße anpassbar. Sie ermöglichen es Ihnen, Benutzeraktivitäten auf Ihren OpenSearch Clustern nachzuverfolgen, einschließlich erfolgreicher und fehlgeschlagener AuthentifizierungenOpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Abhilfe

Anweisungen zur Aktivierung von Audit-Logs finden Sie unter Aktivieren von Audit-Logs im Amazon OpenSearch Service Developer Guide.

[Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-data-node-fault-tolerance`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob OpenSearch Domänen mit mindestens drei Datenknoten konfiguriert sind und `zoneAwarenessEnabled` ist`true`. Dieses Steuerelement schlägt für eine OpenSearch Domäne fehl, wenn sie `instanceCount` weniger als 3 `zoneAwarenessEnabled` ist oder ist`false`.

Für eine OpenSearch Domäne sind mindestens drei Datenknoten erforderlich, um eine hohe Verfügbarkeit und Fehlertoleranz zu gewährleisten. Durch die Bereitstellung einer OpenSearch Domäne mit mindestens drei Datenknoten wird der Clusterbetrieb gewährleistet, falls ein Knoten ausfällt.

Abhilfe

Um die Anzahl der Datenknoten in einer OpenSearch Domäne zu ändern

1. Melden Sie sich bei der AWS Konsole an und öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/.
2. Wählen Sie unter Meine Domains den Namen der zu bearbeitenden Domain aus und klicken Sie auf Bearbeiten.

3. Stellen Sie unter Datenknoten die Anzahl der Knoten auf eine Zahl größer als ein3. Wenn Sie in drei Availability Zones bereitstellen, legen Sie die Zahl auf ein Vielfaches von drei fest, um eine gleichmäßige Verteilung auf die Availability Zones sicherzustellen.
4. Wählen Sie Absenden aus.

Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-5, NIST.800-53.r5 AC-6

Kategorie: Schützen > Sicheres Zugriffsmanagement > Eingeschränkte sensible API-Aktionen

Schweregrad: Hoch

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-access-control-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für OpenSearch Domänen eine differenzierte Zugriffskontrolle aktiviert ist. Die Steuerung schlägt fehl, wenn die feinkörnige Zugriffskontrolle nicht aktiviert ist. Für die differenzierte Zugriffskontrolle muss `advanced-security-options` der OpenSearch Parameter `update-domain-config` aktiviert sein.

Eine detaillierte Zugriffskontrolle bietet zusätzliche Möglichkeiten, den Zugriff auf Ihre Daten bei Amazon OpenSearch Service zu kontrollieren.

Abhilfe

Informationen zur Aktivierung der feinkörnigen Zugriffskontrolle finden Sie unter Feinkörnige Zugriffskontrolle in Amazon OpenSearch Service im Amazon OpenSearch Service Developer Guide.

[Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.R5 AC-17 (2), NIST.800-53.R5 AC-4, NIST.800-53.R5 IA-5 (1), NIst.800-53.R5 SC-12 (3), NIst.800-53.R5 SC-13, NIst.800-53.R5 SC-23, NIst.800-53.R5

SC-23 (3), NIst.NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategorie: Schützen > Datenschutz > Verschlüsselung von data-in-transit

Schweregrad: Mittel

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-https-required`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10`(nicht anpassbar)

Diese Steuerung prüft, ob ein Amazon OpenSearch Service-Domain-Endpunkt so konfiguriert ist, dass er die neueste TLS-Sicherheitsrichtlinie verwendet. Die Kontrolle schlägt fehl, wenn der OpenSearch Domain-Endpunkt nicht für die Verwendung der neuesten unterstützten Richtlinie konfiguriert ist oder wenn HTTPS nicht aktiviert ist.

HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer person-in-the-middle oder ähnliche Angriffe verwenden, um den Netzwerkverkehr zu belauschen oder zu manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Die Verschlüsselung von Daten während der Übertragung kann die Leistung beeinträchtigen. Sie sollten Ihre Anwendung mit dieser Funktion testen, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen. TLS 1.2 bietet mehrere Sicherheitsverbesserungen gegenüber früheren Versionen von TLS.

Abhilfe

Verwenden Sie den UpdateDomainConfigAPI-Vorgang, um die TLS-Verschlüsselung zu aktivieren. Konfigurieren Sie das DomainEndpointOptionsFeld, um das festzulegen`TLSSecurityPolicy`. Weitere Informationen finden Sie unter ode-to-node N-Verschlüsselung im Amazon OpenSearch Service Developer Guide.

[Opensearch.9] OpenSearch -Domains sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config Regel: `tagged-opensearch-domain` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob eine Amazon OpenSearch Service-Domain Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die Domain keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Domain mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen

möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer OpenSearch Service-Domain finden Sie unter Arbeiten mit Tags im Amazon OpenSearch Service Developer Guide.

Auf [Opensearch.10] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein

Verwandte Anforderungen: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIst.800-53.R5 SI-2 (5)

Kategorie: Erkennen > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Niedrig

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-update-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob auf einer Amazon OpenSearch Service-Domain das neueste Softwareupdate installiert ist. Die Kontrolle schlägt fehl, wenn ein Softwareupdate verfügbar, aber nicht für die Domain installiert ist.

OpenSearch Service-Softwareupdates bieten die neuesten Plattformkorrekturen, Updates und Funktionen, die für die Umgebung verfügbar sind. Die up-to-date Beibehaltung der Patch-Installation trägt dazu bei, die Sicherheit und Verfügbarkeit der Domain aufrechtzuerhalten. Wenn bei den

erforderlichen Updates keine Maßnahmen ergriffen werden, wird die Service-Software automatisch aktualisiert (in der Regel nach 2 Wochen). Wir empfehlen, Updates in Zeiten mit geringem Datenverkehr auf der Domain zu planen, um Betriebsunterbrechungen zu minimieren.

Abhilfe

Informationen zur Installation von Softwareupdates für eine OpenSearch Domain finden Sie unter Ein Update starten im Amazon OpenSearch Service Developer Guide.

[Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-2, NIST.800-53.R5 SC-5, NIST.800-53.R5 SC-36, NIST.800-53.R5 SI-13

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::OpenSearch::Domain`

AWS Config -Regel: `opensearch-primary-node-fault-tolerance`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob eine Amazon OpenSearch Service-Domain mit mindestens drei dedizierten Primärknoten konfiguriert ist. Die Kontrolle schlägt fehl, wenn die Domain weniger als drei dedizierte Primärknoten hat.

OpenSearch Der Dienst verwendet dedizierte Primärknoten, um die Clusterstabilität zu erhöhen. Ein dedizierter primärer Knoten führt Clusterverwaltungsaufgaben aus, speichert jedoch keine Daten und reagiert auch nicht auf Anfragen zum Hochladen von Daten. Wir empfehlen die Verwendung von Multi-AZ mit Standby, wodurch jeder OpenSearch Produktionsdomäne drei dedizierte Primärknoten hinzugefügt werden.

Abhilfe

Informationen zum Ändern der Anzahl der Primärknoten für eine OpenSearch Domain finden Sie unter Erstellen und Verwalten von Amazon OpenSearch Service-Domains im Amazon OpenSearch Service Developer Guide.

AWS Private Certificate Authority steuert

Diese Kontrollen beziehen sich auf AWS Private CA Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[PCA.1] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Niedrig

Art der Ressource: `AWS::ACMPCA::CertificateAuthority`

AWS Config -Regel: `acm-pca-root-ca-disabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob es AWS Private CA eine deaktivierte Stammzertifizierungsstelle (CA) gibt. Die Steuerung schlägt fehl, wenn die Stammzertifizierungsstelle aktiviert ist.

Mit AWS Private CA können Sie eine Zertifizierungsstellenhierarchie erstellen, die eine Stammzertifizierungsstelle und untergeordnete Zertifizierungsstellen umfasst. Sie sollten die Verwendung der Stammzertifizierungsstelle für tägliche Aufgaben minimieren, insbesondere in Produktionsumgebungen. Die Stammzertifizierungsstelle sollte nur zur Ausstellung von Zertifikaten für zwischengeschaltete Zertifizierungsstellen verwendet werden. Dadurch kann die Stammzertifizierungsstelle gespeichert werden, ohne Schaden zu nehmen, während die Zwischenzertifizierungsstellen das tägliche Ausstellen von Endentitätszertifikaten übernehmen.

Abhilfe

Informationen zum Deaktivieren der Root-CA finden Sie unter CA-Status aktualisieren im AWS Private Certificate Authority Benutzerhandbuch.

Steuerelemente von Amazon Relational Database Service

Diese Kontrollen beziehen sich auf Amazon RDS-Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[RDS.1] Der RDS-Snapshot sollte privat sein

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.R5 AC-21, NIST.800-53.r5 AC-3, NIst.800-53.r5 AC-3 (7), NIST.800-53.R5 AC-3 R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21)), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Ressourcentyp:`AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

AWS Config -Regel: `rds-snapshots-public-prohibited`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon RDS-Snapshots öffentlich sind. Die Steuerung schlägt fehl, wenn RDS-Snapshots öffentlich sind. Dieses Steuerelement bewertet RDS-Instances, Aurora-DB-Instances, Neptune-DB-Instances und Amazon DocumentDB-Cluster.

RDS-Snapshots werden verwendet, um die Daten auf Ihren RDS-Instances zu einem bestimmten Zeitpunkt zu sichern. Sie können verwendet werden, um frühere Zustände von RDS-Instances wiederherzustellen.

Ein RDS-Snapshot darf nur öffentlich sein, wenn dies beabsichtigt ist. Wenn Sie einen unverschlüsselten manuellen Snapshot als öffentlich freigeben, wird der Snapshot dadurch für alle verfügbar. AWS-Konten Dies kann zu einer unbeabsichtigten Offenlegung von Daten Ihrer RDS-Instance führen.

Beachten Sie, dass die AWS Config Regel die Änderung möglicherweise bis zu 12 Stunden lang nicht erkennen kann, wenn die Konfiguration so geändert wird, dass sie öffentlich zugänglich ist. Bis die AWS Config Regel die Änderung erkennt, ist die Prüfung erfolgreich, obwohl die Konfiguration gegen die Regel verstößt.

Weitere Informationen zum Teilen eines DB-Snapshots finden Sie unter Freigeben eines DB-Snapshots im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Entfernen des öffentlichen Zugriffs auf RDS-Snapshots finden Sie unter Einen Snapshot teilen im Amazon RDS-Benutzerhandbuch. Für die Sichtbarkeit von DB-Snapshots wählen wir Privat.

[RDS.2] RDS-DB-Instances sollten je nach Dauer den öffentlichen Zugriff verbieten PubliclyAccessible AWS Config

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/2.3.3, PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (5)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-instance-public-access-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon RDS-Instances öffentlich zugänglich sind, indem es das `PubliclyAccessible` Feld im Instance-Konfigurationselement auswertet.

Neptune-DB-Instances und Amazon DocumentDB-Cluster haben das `PubliclyAccessible` Flag nicht und können nicht ausgewertet werden. Diese Kontrolle kann jedoch immer noch Ergebnisse für diese Ressourcen generieren. Sie können diese Ergebnisse unterdrücken.

Der `PubliclyAccessible`-Wert in der RDS-Instance-Konfiguration gibt an, ob die DB-Instance öffentlich zugänglich ist. Wenn die DB-Instance mit `PubliclyAccessible` konfiguriert ist, handelt es sich um eine mit dem Internet verbundene Instance mit einem öffentlich auflösbaren DNS-Namen,

der in eine öffentliche IP-Adresse aufgelöst wird. Wenn die DB-Instance nicht öffentlich zugänglich ist, handelt es sich um eine interne Instance mit einem DNS-Namen, der in eine private IP-Adresse aufgelöst wird.

Sofern Sie nicht beabsichtigen, dass Ihre RDS-Instance öffentlich zugänglich ist, sollte die RDS-Instance nicht mit `PubliclyAccessible` Value konfiguriert werden. Dadurch könnte unnötiger Datenverkehr zu Ihrer Datenbank-Instance entstehen.

Abhilfe

Informationen zum Entfernen des öffentlichen Zugriffs auf RDS-DB-Instances finden Sie unter Ändern einer Amazon RDS-DB-Instance im Amazon RDS-Benutzerhandbuch. Wählen Sie für öffentlichen Zugriff die Option Nein.

[RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/2.3.1, CIS AWS Foundations Benchmark v1.4.0/2.3.1, NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIst.800-53.R5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-storage-encrypted`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob die Speicherverschlüsselung für Ihre Amazon RDS-DB-Instances aktiviert ist.

Diese Steuerung ist für RDS-DB-Instances vorgesehen. Es kann jedoch auch Ergebnisse für Aurora-DB-Instances, Neptune-DB-Instances und Amazon DocumentDB-Cluster generieren. Wenn diese Ergebnisse nicht nützlich sind, können Sie sie unterdrücken.

Um eine zusätzliche Sicherheitsebene für Ihre sensiblen Daten in RDS-DB-Instances zu erhalten, sollten Sie Ihre RDS-DB-Instances so konfigurieren, dass sie im Ruhezustand verschlüsselt werden. Um Ihre RDS-DB-Instances und Snapshots im Ruhezustand zu verschlüsseln, aktivieren Sie die Verschlüsselungsoption für Ihre RDS-DB-Instances. Daten, die im Ruhezustand verschlüsselt werden, umfassen den zugehörigen Speicherplatz für DB-Instances, deren automatisierte Backups, Read Replicas und Snapshots.

RDS-verschlüsselte DB-Instances verwenden den offenen Standard AES-256-Verschlüsselungsalgorithmus, um Ihre Daten auf dem Server zu verschlüsseln, der Ihre RDS-DB-Instance hostet. Nachdem Ihre Daten verschlüsselt wurden, verarbeitet Amazon RDS die Authentifizierung des Zugriffs und die Entschlüsselung Ihrer Daten transparent und mit minimalen Auswirkungen auf die Leistung. Sie müssen Ihre Datenbank-Client-Anwendungen nicht ändern, um die Verschlüsselung anzuwenden.

Die Amazon RDS-Verschlüsselung ist derzeit für alle Datenbank-Engines und Speichertypen verfügbar. Amazon RDS-Verschlüsselung ist für die meisten DB-Instance-Klassen verfügbar. Informationen zu DB-Instance-Klassen, die die Amazon RDS-Verschlüsselung nicht unterstützen, finden Sie unter Verschlüsseln von Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zur Verschlüsselung von DB-Instances in Amazon RDS finden Sie unter Verschlüsseln von Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.

[RDS.4] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Ressourcentyp:`AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

AWS Config -Regel: `rds-snapshot-encrypted`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein RDS-DB-Snapshot verschlüsselt ist. Die Steuerung schlägt fehl, wenn ein RDS-DB-Snapshot nicht verschlüsselt ist.

Dieses Steuerelement ist für RDS-DB-Instances vorgesehen. Es kann jedoch auch Ergebnisse für Snapshots von Aurora-DB-Instances, Neptune-DB-Instances und Amazon DocumentDB-Clustern generieren. Wenn diese Ergebnisse nicht nützlich sind, können Sie sie unterdrücken.

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass ein nicht authentifizierter Benutzer Zugriff auf Daten erhält, die auf der Festplatte gespeichert sind. Daten in RDS-Snapshots sollten im Ruhezustand verschlüsselt werden, um eine zusätzliche Sicherheitsebene zu gewährleisten.

Abhilfe

Informationen zum Verschlüsseln eines RDS-Snapshots finden Sie unter Verschlüsseln von Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch. Wenn Sie eine RDS-DB-Instance verschlüsseln, umfassen die verschlüsselten Daten den der Instance zugrunde liegenden Speicher, ihre automatisierten Backups, Read Replicas und Snapshots.

Sie können eine RDS-DB-Instance nur verschlüsseln, wenn Sie sie erstellen, nicht nachdem die DB-Instance erstellt wurde. Da es jedoch möglich ist, die Kopie eines unverschlüsselten Snapshots zu verschlüsseln, können Sie quasi eine Verschlüsselung zu einer unverschlüsselten DB-Instance hinzufügen. Dies lässt sich durchführen, indem Sie einen Snapshot von Ihrer DB-Instance erstellen und dann eine verschlüsselte Kopie dieses Snapshots erstellen. Anschließend können Sie Ihre DB-Instance aus dem verschlüsselten Snapshot wiederherstellen und verfügen so über eine verschlüsselte Kopie Ihrer ursprünglichen DB-Instance.

[RDS.5] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-multi-az-support`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Hochverfügbarkeit für Ihre RDS-DB-Instances aktiviert ist.

RDS-DB-Instances sollten für mehrere Availability Zones (AZs) konfiguriert werden. Dadurch wird die Verfügbarkeit der gespeicherten Daten gewährleistet. Multi-AZ-Bereitstellungen ermöglichen einen automatisierten Failover bei Problemen mit der AZ-Verfügbarkeit und während der regulären RDS-Wartung.

Abhilfe

Um Ihre DB-Instances in mehreren AZs bereitzustellen, finden Sie unter Ändern einer DB-Instance zu einer Multi-AZ-DB-Instance-Bereitstellung im Amazon RDS-Benutzerhandbuch.

[RDS.6] Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden

Verwandte Anforderungen: NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-2

Kategorie: Erkennung > Erkennungsservices

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-enhanced-monitoring-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert	
`monitoringInterval`	Anzahl der Sekunden zwischen den Intervall	Enum	`1`, `5`, `10`, `15`, `30`, `60`	Kein Standardwert	

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	en zur Erfassung von Überwachungsmetriken			

Dieses Steuerelement prüft, ob die erweiterte Überwachung für eine Amazon Relational Database Service (Amazon RDS) -DB-Instance aktiviert ist. Die Steuerung schlägt fehl, wenn die erweiterte Überwachung für die Instance nicht aktiviert ist. Wenn Sie einen benutzerdefinierten Wert für den `monitoringInterval` Parameter angeben, ist die Steuerung nur erfolgreich, wenn die Metriken zur erweiterten Überwachung für die Instance im angegebenen Intervall erfasst werden.

In Amazon RDS ermöglicht Enhanced Monitoring eine schnellere Reaktion auf Leistungsänderungen in der zugrunde liegenden Infrastruktur. Diese Leistungsänderungen können zu einer mangelnden Verfügbarkeit der Daten führen. Enhanced Monitoring bietet Echtzeit-Metriken des Betriebssystems, auf dem Ihre RDS-DB-Instance läuft. Auf der Instance ist ein Agent installiert. Der Agent kann Metriken genauer abrufen, als dies auf der Hypervisor-Ebene möglich ist.

Metriken von Enhanced Monitoring sind nützlich, um zu sehen, wie unterschiedliche Prozesse oder Threads auf einer DB-Instance die CPU nutzen. Weitere Informationen finden Sie unter Enhanced Monitoring (Erweiterte Überwachung) im Amazon-RDS-Benutzerhandbuch.

Abhilfe

Detaillierte Anweisungen zur Aktivierung von Enhanced Monitoring für Ihre DB-Instance finden Sie unter Enhanced Monitoring einrichten und aktivieren im Amazon RDS-Benutzerhandbuch.

[RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CM-3, NIST.800-53.R5 SC-5 (2)

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `rds-cluster-deletion-protection-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen RDS-DB-Cluster der Löschschutz aktiviert ist. Die Steuerung schlägt fehl, wenn für einen RDS-DB-Cluster kein Löschschutz aktiviert ist.

Dieses Steuerelement ist für RDS-DB-Instances vorgesehen. Es kann jedoch auch Ergebnisse für Aurora-DB-Instances, Neptune-DB-Instances und Amazon DocumentDB-Cluster generieren. Wenn diese Ergebnisse nicht nützlich sind, können Sie sie unterdrücken.

Die Aktivierung des Cluster-Löschschutzes bietet zusätzlichen Schutz vor versehentlichem Löschen von Datenbanken oder vor dem Löschen durch eine nicht autorisierte Entität.

Wenn der Löschschutz aktiviert ist, kann ein RDS-Cluster nicht gelöscht werden. Bevor eine Löschanforderung erfolgreich sein kann, muss der Löschschutz deaktiviert werden.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für einen RDS-DB-Cluster finden Sie unter Ändern des DB-Clusters mithilfe der Konsole, der CLI und der API im Amazon RDS-Benutzerhandbuch. Wählen Sie für den Löschschutz die Option Löschschutz aktivieren.

[RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CM-3, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-instance-deletion-protection-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `databaseEngines`: `mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web` (nicht anpassbar)

Dieses Steuerelement prüft, ob für Ihre RDS-DB-Instances, die eine der aufgelisteten Datenbank-Engines verwenden, der Löschschutz aktiviert ist. Die Steuerung schlägt fehl, wenn für eine RDS-DB-Instance kein Löschschutz aktiviert ist.

Die Aktivierung des Schutzes vor dem Löschen von Instances ist eine zusätzliche Schutzebene gegen das versehentliche Löschen von Datenbanken oder das Löschen durch eine nicht autorisierte Entität.

Solange der Löschschutz aktiviert ist, kann eine RDS-DB-Instance nicht gelöscht werden. Bevor eine Löschanforderung erfolgreich sein kann, muss der Löschschutz deaktiviert werden.

Abhilfe

Informationen zum Aktivieren des Löschschutzes für eine RDS-DB-Instance finden Sie unter Ändern einer Amazon RDS-DB-Instance im Amazon RDS-Benutzerhandbuch. Wählen Sie für den Löschschutz die Option Löschschutz aktivieren.

[RDS.9] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.r5 AU-3 R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-3 (8), NIst.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-4 (20) R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-logging-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon RDS-DB-Instance so konfiguriert ist, dass sie die folgenden Protokolle in Amazon CloudWatch Logs veröffentlicht. Die Kontrolle schlägt fehl, wenn die Instance nicht so konfiguriert ist, dass sie die folgenden CloudWatch Protokolle in Logs veröffentlicht:

- Oracle: (Alert, Audit, Trace, Listener)

- PostgreSQL: (Postgresql, Aktualisierung)
- MySQL: (Prüfung, Fehler, Allgemein, SlowQuery)
- MariaDB: (Prüfung, Fehler, Allgemein,) SlowQuery
- SQL Server: (Fehler, Agent)
- Aurora: (Prüfung, Fehler, Allgemein, SlowQuery)
- Aurora-MySQL: (Prüfung, Fehler, Allgemein,) SlowQuery
- Aurora-PostgreSQL: (Postgresql, Aktualisierung).

Für RDS-Datenbanken sollten die entsprechenden Protokolle aktiviert sein. Die Datenbankprotokollierung bietet detaillierte Aufzeichnungen der an RDS gestellten Anfragen. Datenbankprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Abhilfe

Informationen zum Veröffentlichen von CloudWatch RDS-Datenbankprotokollen in Logs finden Sie unter Angeben der in CloudWatch Logs zu veröffentlichenden Logs im Amazon RDS-Benutzerhandbuch.

[RDS.10] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-6

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-instance-iam-authentication-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine RDS-DB-Instance die IAM-Datenbankauthentifizierung aktiviert ist. Die Steuerung schlägt fehl, wenn die IAM-Authentifizierung nicht für RDS-DB-Instances konfiguriert ist. Diese Steuerung bewertet nur RDS-Instances mit den folgenden Engine-

Typen:`mysql`,`postgres`,, `aurora` `aurora-mysql`aurora-postgresql, und. `mariadb` Eine RDS-Instanz muss sich außerdem in einem der folgenden Zustände befinden, damit ein Ergebnis generiert werden kann:`available`, `backing-upstorage-optimization`, oder`storage-full`.

Die IAM-Datenbankauthentifizierung ermöglicht die Authentifizierung von Datenbank-Instances mit einem Authentifizierungstoken anstelle eines Kennworts. Der Netzwerkverkehr zur und von der Datenbank wird mit SSL verschlüsselt. Weitere Informationen finden Sie unter IAM-Datenbank-Authentifizierung im Amazon Aurora-Benutzerhandbuch.

Abhilfe

Informationen zur Aktivierung der IAM-Datenbankauthentifizierung auf einer RDS-DB-Instance finden Sie unter Aktivieren und Deaktivieren der IAM-Datenbankauthentifizierung im Amazon RDS-Benutzerhandbuch.

[RDS.11] Bei RDS-Instances sollten automatische Backups aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6, NIST.800-53.R5 CP-6 (1), NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 CP-9, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellen > Resilienz > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: `AWS::RDS::DBInstance`

AWS Config -Regel: `db-instance-backup-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert	
`backupRetentionMinimum`	Minimale Aufbewahrungsdauer für Backups in Tagen	Ganzzahl	7 auf 35	7	

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert	
`checkReadReplicas`	Überprüft, ob für RDS-DB-Instances Backups für Read Replicas aktiviert sind	Boolesch	Nicht anpassbar	`false`	

Diese Kontrolle prüft, ob für eine Amazon Relational Database Service Service-Instance automatische Backups aktiviert sind und ob eine Aufbewahrungsfrist für Backups größer oder gleich dem angegebenen Zeitraum ist. Read Replicas sind von der Evaluierung ausgeschlossen. Die Kontrolle schlägt fehl, wenn Backups für die Instanz nicht aktiviert sind oder wenn die Aufbewahrungsdauer unter dem angegebenen Zeitraum liegt. Sofern Sie keinen benutzerdefinierten Parameterwert für die Aufbewahrungsdauer von Backups angeben, verwendet Security Hub einen Standardwert von 7 Tagen.

Backups helfen Ihnen, sich schneller nach einem Sicherheitsvorfall zu erholen, und stärken die Widerstandsfähigkeit Ihrer Systeme. Mit Amazon RDS können Sie tägliche Snapshots des gesamten Instance-Volumes konfigurieren. Weitere Informationen zu automatisierten Amazon RDS-Backups finden Sie unter Arbeiten mit Backups im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Aktivieren automatisierter Backups auf einer RDS-DB-Instance finden Sie unter Automatisierte Backups aktivieren im Amazon RDS-Benutzerhandbuch.

[RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-6

Kategorie: Schützen > Sichere Zugriffsverwaltung > Passwortlose Authentifizierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `rds-cluster-iam-authentication-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem Amazon RDS-DB-Cluster die IAM-Datenbankauthentifizierung aktiviert ist.

Die IAM-Datenbankauthentifizierung ermöglicht eine passwortlose Authentifizierung bei Datenbank-Instances. Die Authentifizierung verwendet ein Authentifizierungstoken. Der Netzwerkverkehr zur und von der Datenbank wird mit SSL verschlüsselt. Weitere Informationen finden Sie unter IAM-Datenbank-Authentifizierung im Amazon Aurora-Benutzerhandbuch.

Abhilfe

Informationen zur Aktivierung der IAM-Authentifizierung für einen DB-Cluster finden Sie unter Aktivieren und Deaktivieren der IAM-Datenbankauthentifizierung im Amazon Aurora Aurora-Benutzerhandbuch.

[RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/2.3.2, NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIst.800-53.R5 SI-2 (4), NIST.800-53.R5 SI-2 (5)

Kategorie: Erkennen > Sicherheitslücken- und Patch-Management

Schweregrad: Hoch

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-automatic-minor-version-upgrade-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob automatische Upgrades für kleinere Versionen für die RDS-Datenbank-Instance aktiviert sind.

Durch die Aktivierung automatischer Nebenversions-Upgrades wird sichergestellt, dass die neuesten Updates für die Nebenversionen des relationalen Datenbankmanagementsystems (RDBMS) installiert werden. Diese Upgrades können Sicherheitspatches und Bugfixes beinhalten. Es ist ein wichtiger Schritt zur Sicherung von Systemen, über die Installation von Patches auf dem Laufenden zu bleiben.

Abhilfe

Informationen zur Aktivierung automatischer Unterversions-Upgrades für eine bestehende DB-Instance finden Sie unter Ändern einer Amazon RDS-DB-Instance im Amazon RDS-Benutzerhandbuch. Wählen Sie für das automatische Upgrade der Nebenversion Ja aus.

[RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6, NIST.800-53.R5 CP-6 (1), NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 CP-9, NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: `AWS::RDS::DBCluster`

AWS Config -Regel: `aurora-mysql-backtracking-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert	
`BacktrackWindowInHours`	Anzahl der Stunden, um einen Aurora MySQL-Cluster zurückzuverfolgen	Double	`0.1` auf `72`	Kein Standardwert	

Dieses Steuerelement prüft, ob für einen Amazon Aurora Aurora-Cluster Backtracking aktiviert ist. Die Steuerung schlägt fehl, wenn für den Cluster kein Backtracking aktiviert ist. Wenn Sie einen benutzerdefinierten Wert für den `BacktrackWindowInHours` Parameter angeben, ist die Steuerung nur erfolgreich, wenn der Cluster für den angegebenen Zeitraum zurückverfolgt wird.

Mithilfe von Backups können Sie sich nach einem Sicherheitsvorfall schneller erholen. Sie stärken auch die Widerstandsfähigkeit Ihrer Systeme. Aurora-Backtracking reduziert die Zeit

für die Wiederherstellung einer Datenbank auf einen bestimmten Zeitpunkt. Dazu ist keine Datenbankwiederherstellung erforderlich.

Abhilfe

Informationen zur Aktivierung von Aurora-Backtracking finden Sie unter Backtracking konfigurieren im Amazon Aurora Aurora-Benutzerhandbuch.

Beachten Sie, dass Sie Backtracking nicht auf einem vorhandenen Cluster aktivieren können. Stattdessen können Sie einen Clone erstellen, für den Backtracking aktiviert ist. Weitere Informationen zu den Einschränkungen von Aurora-Backtracking finden Sie in der Liste der Einschränkungen unter Backtracking im Überblick.

[RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 SC-36, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `rds-cluster-multi-az-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Hochverfügbarkeit für Ihre RDS-DB-Cluster aktiviert ist. Die Steuerung schlägt fehl, wenn ein RDS-DB-Cluster nicht in mehreren Availability Zones (AZs) bereitgestellt wird.

RDS-DB-Cluster sollten für mehrere AZs konfiguriert werden, um die Verfügbarkeit der gespeicherten Daten sicherzustellen. Die Bereitstellung auf mehreren AZs ermöglicht einen automatisierten Failover im Falle eines AZ-Verfügbarkeitsproblems und während regelmäßiger RDS-Wartungsereignisse.

Abhilfe

Um Ihre DB-Cluster in mehreren AZs bereitzustellen, finden Sie unter Ändern einer DB-Instance zu einer Multi-AZ-DB-Instance-Bereitstellung im Amazon RDS-Benutzerhandbuch.

Die Schritte zur Behebung sind für globale Aurora-Datenbanken unterschiedlich. Um mehrere Availability Zones für eine globale Aurora-Datenbank zu konfigurieren, wählen Sie Ihren DB-Cluster aus. Wählen Sie dann Aktionen und Leser hinzufügen und geben Sie mehrere AZs an. Weitere Informationen finden Sie unter Hinzufügen von Aurora Replicas zu einem DB-Cluster im Amazon Aurora Aurora-Benutzerhandbuch.

[RDS.16] RDS-DB-Cluster sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.r5 CM-2 (2)

Kategorie: Identifizieren > Bestand

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config Regel: `rds-cluster-copy-tags-to-snapshots-enabled` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob RDS-DB-Cluster so konfiguriert sind, dass bei der Erstellung der Snapshots alle Tags in Snapshots kopiert werden.

Die Identifizierung und Inventarisierung Ihrer IT-Ressourcen ist ein entscheidender Aspekt der Unternehmensführung und Sicherheit. Sie benötigen einen Überblick über all Ihre RDS-DB-Cluster, damit Sie deren Sicherheitslage beurteilen und Maßnahmen gegen potenzielle Schwachstellen ergreifen können. Snapshots sollten auf die gleiche Weise gekennzeichnet werden wie ihre übergeordneten RDS-Datenbankcluster. Durch die Aktivierung dieser Einstellung wird sichergestellt, dass Snapshots die Tags ihrer übergeordneten Datenbankcluster erben.

Abhilfe

Informationen zum automatischen Kopieren von Tags in Snapshots für einen RDS-DB-Cluster finden Sie unter Ändern des DB-Clusters mithilfe der Konsole, der CLI und der API im Amazon Aurora Aurora-Benutzerhandbuch. Wählen Sie Tags in Snapshots kopieren aus.

[RDS.17] RDS-DB-Instances sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.r5 CM-2 (2)

Kategorie: Identifizieren > Bestand

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config Regel: `rds-instance-copy-tags-to-snapshots-enabled` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob RDS-DB-Instances so konfiguriert sind, dass sie bei der Erstellung der Snapshots alle Tags in Snapshots kopieren.

Die Identifizierung und Inventarisierung Ihrer IT-Ressourcen ist ein entscheidender Aspekt der Unternehmensführung und Sicherheit. Sie benötigen einen Überblick über all Ihre RDS-DB-Instances, damit Sie deren Sicherheitslage beurteilen und Maßnahmen gegen potenzielle Schwachstellen ergreifen können. Snapshots sollten auf die gleiche Weise gekennzeichnet werden wie ihre übergeordneten RDS-Datenbank-Instances. Durch die Aktivierung dieser Einstellung wird sichergestellt, dass Snapshots die Tags ihrer übergeordneten Datenbank-Instances erben.

Abhilfe

Informationen zum automatischen Kopieren von Tags in Snapshots für eine RDS-DB-Instance finden Sie unter Ändern einer Amazon RDS-DB-Instance im Amazon RDS-Benutzerhandbuch. Wählen Sie Tags in Snapshots kopieren aus.

[RDS.18] RDS-Instances sollten in einer VPC bereitgestellt werden

Verwandte Anforderungen: NIST.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20),

NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Hoch

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config Regel: `rds-deployed-in-vpc` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon RDS-Instance auf einer EC2-VPC bereitgestellt ist.

VPCs bieten eine Reihe von Netzwerksteuerungen, um den Zugriff auf RDS-Ressourcen zu sichern. Zu diesen Kontrollen gehören VPC-Endpunkte, Netzwerk-ACLs und Sicherheitsgruppen. Um diese Kontrollen nutzen zu können, empfehlen wir Ihnen, Ihre RDS-Instances auf einer EC2-VPC zu erstellen.

Abhilfe

Anweisungen zum Verschieben von RDS-Instances in eine VPC finden Sie unter Aktualisieren der VPC für eine DB-Instance im Amazon RDS-Benutzerhandbuch.

[RDS.19] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Cluster-Ereignisse konfiguriert werden

Verwandte Anforderungen: NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-2

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::EventSubscription`

AWS Config Regel: `rds-cluster-event-notifications-configured` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem bestehenden Amazon RDS-Ereignisabonnement für Datenbankcluster Benachrichtigungen für die folgenden Schlüssel-Wert-Paare aus Quelle und Ereigniskategorie aktiviert sind:

```
DBCluster: ["maintenance","failure"]
```

Die Kontrolle ist erfolgreich, wenn in Ihrem Konto keine Event-Abonnements vorhanden sind.

RDS-Ereignisbenachrichtigungen verwendet Amazon SNS, um Sie über Änderungen in der Verfügbarkeit oder Konfiguration Ihrer RDS-Ressourcen zu informieren. Diese Benachrichtigungen ermöglichen eine schnelle Reaktion. Weitere Informationen zu RDS-Ereignisbenachrichtigungen finden Sie unter Verwenden von Amazon RDS-Ereignisbenachrichtigungen im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Abonnieren von RDS-Cluster-Ereignisbenachrichtigungen finden Sie unter Amazon RDS-Ereignisbenachrichtigungen abonnieren im Amazon RDS-Benutzerhandbuch. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Source type (Quellentyp)	Cluster
Zu berücksichtigende Cluster	Alle Cluster
Zu berücksichtigende Veranstaltungskategorien	Wählen Sie bestimmte Veranstaltungskategorien oder Alle Veranstaltungskategorien

[RDS.20] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden

Verwandte Anforderungen: NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-2

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::EventSubscription`

AWS Config Regel: `rds-instance-event-notifications-configured` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob in einem bestehenden Amazon RDS-Ereignisabonnement für Datenbank-Instances Benachrichtigungen für die folgenden Schlüssel-Wert-Paare aus Quelltyp und Ereigniskategorie aktiviert sind:

```
DBInstance: ["maintenance","configuration change","failure"]
```

Die Kontrolle ist erfolgreich, wenn in Ihrem Konto keine Event-Abonnements vorhanden sind.

RDS-Ereignisbenachrichtigungen verwenden Amazon SNS, um Sie über Änderungen in der Verfügbarkeit oder Konfiguration Ihrer RDS-Ressourcen zu informieren. Diese Benachrichtigungen ermöglichen eine schnelle Reaktion. Weitere Informationen zu RDS-Ereignisbenachrichtigungen finden Sie unter Verwenden von Amazon RDS-Ereignisbenachrichtigungen im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Abonnieren von RDS-Instance-Ereignisbenachrichtigungen finden Sie unter Amazon RDS-Ereignisbenachrichtigungen abonnieren im Amazon RDS-Benutzerhandbuch. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Source type (Quellentyp)	Instances
Instances, die aufgenommen werden sollen	Alle Instanzen
Zu berücksichtigende Event-Kategorien	Wählen Sie bestimmte Veranstaltungskategorien oder Alle Veranstaltungskategorien

[RDS.21] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankparametergruppenereignisse konfiguriert werden

Verwandte Anforderungen: NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-2

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::EventSubscription`

AWS Config Regel: `rds-pg-event-notifications-configured` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon RDS-Ereignisabonnement mit aktivierten Benachrichtigungen für die folgenden Schlüsselwertpaare aus Quelltyp, Ereigniskategorie, aktiviert ist.

```
DBParameterGroup: ["configuration change"]
```

RDS-Ereignisbenachrichtigungen verwenden Amazon SNS, um Sie über Änderungen in der Verfügbarkeit oder Konfiguration Ihrer RDS-Ressourcen zu informieren. Diese Benachrichtigungen ermöglichen eine schnelle Reaktion. Weitere Informationen zu RDS-Ereignisbenachrichtigungen finden Sie unter Verwenden von Amazon RDS-Ereignisbenachrichtigungen im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Abonnieren von Ereignisbenachrichtigungen für RDS-Datenbankparametergruppen finden Sie unter Amazon RDS-Ereignisbenachrichtigungen abonnieren im Amazon RDS-Benutzerhandbuch. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Source type (Quellentyp)	Parametergruppen
Zu berücksichtigende Parametergruppen	Alle Parametergruppen
Zu berücksichtigende Event-Kategorien	Wählen Sie bestimmte Veranstaltungskategorien oder Alle Veranstaltungskategorien

[RDS.22] Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbanksicherheitsgruppenereignisse konfiguriert werden

Verwandte Anforderungen: NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-2

Kategorie: Erkennen > Erkennungsdienste > Anwendungsüberwachung

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::EventSubscription`

AWS Config Regel: `rds-sg-event-notifications-configured` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon RDS-Ereignisabonnement mit aktivierten Benachrichtigungen für die folgenden Schlüsselwertpaare aus Quelltyp, Ereigniskategorie, aktiviert ist.

```
DBSecurityGroup: ["configuration change","failure"]
```

RDS-Ereignisbenachrichtigungen verwenden Amazon SNS, um Sie über Änderungen in der Verfügbarkeit oder Konfiguration Ihrer RDS-Ressourcen zu informieren. Diese Benachrichtigungen ermöglichen eine schnelle Reaktion. Weitere Informationen zu RDS-Ereignisbenachrichtigungen finden Sie unter Verwenden von Amazon RDS-Ereignisbenachrichtigungen im Amazon RDS-Benutzerhandbuch.

Abhilfe

Informationen zum Abonnieren von RDS-Instance-Ereignisbenachrichtigungen finden Sie unter Amazon RDS-Ereignisbenachrichtigungen abonnieren im Amazon RDS-Benutzerhandbuch. Verwenden Sie die folgenden Werte:

Feld	Value (Wert)
Source type (Quellentyp)	Sicherheitsgruppen

Feld	Value (Wert)
Zu berücksichtigende Sicherheitsgruppen	Alle Sicherheitsgruppen
Zu berücksichtigende Event-Kategorien	Wählen Sie bestimmte Veranstaltungskategorien oder Alle Veranstaltungskategorien

[RDS.23] RDS-Instances sollten keinen Standard-Port für die Datenbank-Engine verwenden

Verwandte Anforderungen: NIst.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (5)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config Regel: `rds-no-default-ports` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein RDS-Cluster oder eine RDS-Instanz einen anderen Port als den Standardport der Datenbank-Engine verwendet. Die Steuerung schlägt fehl, wenn der RDS-Cluster oder die RDS-Instanz den Standardport verwendet.

Wenn Sie einen bekannten Port verwenden, um einen RDS-Cluster oder eine RDS-Instanz bereitzustellen, kann ein Angreifer Informationen über den Cluster oder die Instanz erraten. Der Angreifer kann diese Informationen in Verbindung mit anderen Informationen verwenden, um eine Verbindung zu einem RDS-Cluster oder einer RDS-Instance herzustellen oder zusätzliche Informationen über Ihre Anwendung zu erhalten.

Wenn Sie den Port ändern, müssen Sie auch die vorhandenen Verbindungszeichenfolgen aktualisieren, die für die Verbindung mit dem alten Port verwendet wurden. Sie sollten auch die Sicherheitsgruppe der DB-Instance überprüfen, um sicherzustellen, dass sie eine Eingangsregel enthält, die Konnektivität auf dem neuen Port ermöglicht.

Abhilfe

Informationen zum Ändern des Standardports einer vorhandenen RDS-DB-Instance finden Sie unter Ändern einer Amazon RDS-DB-Instance im Amazon RDS-Benutzerhandbuch. Informationen zum Ändern des Standardports eines vorhandenen RDS-DB-Clusters finden Sie unter Ändern des DB-Clusters mithilfe der Konsole, der CLI und der API im Amazon Aurora Aurora-Benutzerhandbuch. Ändern Sie für den Datenbankport den Portwert auf einen Wert, der nicht dem Standard entspricht.

[RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config -Regel: `rds-cluster-default-admin-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon RDS-Datenbank-Cluster den Standardwert des Admin-Benutzernamens geändert hat. Die Steuerung gilt nicht für Engines des Typs Neptune (Neptune DB) oder docdb (DocumentDB). Diese Regel schlägt fehl, wenn der Admin-Benutzername auf den Standardwert gesetzt ist.

Wenn Sie eine Amazon RDS-Datenbank erstellen, sollten Sie den standardmäßigen Administratorbenutzernamen in einen eindeutigen Wert ändern. Standardbenutzernamen sind allgemein bekannt und sollten bei der Erstellung der RDS-Datenbank geändert werden. Durch das Ändern der Standardbenutzernamen wird das Risiko eines unbeabsichtigten Zugriffs verringert.

Abhilfe

Um den Admin-Benutzernamen zu ändern, der mit dem Amazon RDS-Datenbank-Cluster verknüpft ist, erstellen Sie einen neuen RDS-Datenbank-Cluster und ändern Sie den Standard-Admin-Benutzernamen beim Erstellen der Datenbank.

[RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config -Regel: `rds-instance-default-admin-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Sie den Administrator-Benutzernamen für Amazon Relational Database Service (Amazon RDS) -Datenbank-Instances gegenüber dem Standardwert geändert haben. Die Steuerung gilt nicht für Engines des Typs Neptune (Neptune DB) oder docdb (DocumentDB). Die Steuerung schlägt fehl, wenn der Administrator-Benutzername auf den Standardwert gesetzt ist.

Standardmäßige Administratorbenutzernamen in Amazon RDS-Datenbanken sind allgemein bekannt. Wenn Sie eine Amazon RDS-Datenbank erstellen, sollten Sie den standardmäßigen Administratorbenutzernamen in einen eindeutigen Wert ändern, um das Risiko eines unbeabsichtigten Zugriffs zu verringern.

Abhilfe

Um den mit einer RDS-Datenbank-Instance verknüpften Administrator-Benutzernamen zu ändern, erstellen Sie zunächst eine neue RDS-Datenbank-Instance. Ändern Sie den standardmäßigen Administratorbenutzernamen beim Erstellen der Datenbank.

[RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden

Kategorie: Wiederherstellung > Ausfallsicherheit > Backups aktiviert

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6, NIST.800-53.R5 CP-6 (1), NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 CP-9, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-12, NIST.800-53.R5 SI-13 (5)

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config Regel: **`rds-resources-protected-by-backup-plan`**

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert	
`backupVaultLockCheck`	Das Steuerelement gibt einen `PASSED` Befund aus, wenn der Parameter auf true gesetzt ist und die Ressource AWS Backup Vault Lock verwendet.	Boolesch	`true` oder `false`	Kein Standardwert	

Diese Kontrolle bewertet, ob Amazon RDS-DB-Instances durch einen Backup-Plan abgedeckt sind. Diese Kontrolle schlägt fehl, wenn die RDS-DB-Instance nicht durch einen Backup-Plan abgedeckt ist. Wenn Sie den `backupVaultLockCheck` Parameter auf gleich setzen`true`, wird die Kontrolle nur erfolgreich ausgeführt, wenn die Instance in einem AWS Backup gesperrten Tresor gesichert ist.

AWS Backup ist ein vollständig verwalteter Backup-Service, der die gesamte Datensicherung zentralisiert und automatisiert. AWS-Services Mit können Sie Backup-Richtlinien erstellen AWS Backup, die als Backup-Pläne bezeichnet werden. Mit diesen Plänen können Sie Ihre Sicherungsanforderungen definieren, z. B. wie häufig Ihre Daten gesichert werden sollen und wie lange diese Sicherungen aufbewahrt werden sollen. Durch die Aufnahme von RDS-DB-Instances in einen Backup-Plan können Sie Ihre Daten vor unbeabsichtigtem Verlust oder Löschung schützen.

Abhilfe

Informationen zum Hinzufügen einer RDS-DB-Instance zu einem AWS Backup Backup-Plan finden Sie unter Zuweisen von Ressourcen zu einem Backup-Plan im AWS Backup Entwicklerhandbuch.

[RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config Regel: **`rds-cluster-encrypted-at-rest`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein RDS-DB-Cluster im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn ein RDS-DB-Cluster im Ruhezustand nicht verschlüsselt ist.

Daten im Ruhezustand beziehen sich auf alle Daten, die für einen beliebigen Zeitraum in einem persistenten, nichtflüchtigen Speicher gespeichert werden. Durch Verschlüsselung können Sie die Vertraulichkeit solcher Daten schützen und so das Risiko verringern, dass ein unberechtigter Benutzer darauf zugreifen kann. Die Verschlüsselung Ihrer RDS-DB-Cluster schützt Ihre Daten und Metadaten vor unbefugtem Zugriff. Es erfüllt auch die Compliance-Anforderungen für die data-at-rest Verschlüsselung von Produktionsdateisystemen.

Abhilfe

Sie können die Verschlüsselung im Ruhezustand aktivieren, wenn Sie einen RDS-DB-Cluster erstellen. Sie können die Verschlüsselungseinstellungen nach dem Erstellen eines Clusters nicht ändern. Weitere Informationen finden Sie unter Verschlüsseln eines Amazon Aurora Aurora-DB-Clusters im Amazon Aurora Aurora-Benutzerhandbuch.

[RDS.28] RDS-DB-Cluster sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config Regel: `tagged-rds-dbcluster` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon RDS-DB-Cluster Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der DB-Cluster keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der DB-Cluster mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem RDS-DB-Cluster finden Sie unter Tagging Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.

[RDS.29] RDS-DB-Cluster-Snapshots sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBClusterSnapshot`

AWS Config Regel: `tagged-rds-dbclustersnapshot` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlü	StringList	Liste der Tags, die die AWS	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	sseln wird zwischen Groß- und Kleinschreibung unterschieden.		Anforderungen erfüllen	

Dieses Steuerelement prüft, ob ein Amazon RDS-DB-Cluster-Snapshot Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der DB-Cluster-Snapshot keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der DB-Cluster-Snapshot mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem RDS-DB-Cluster-Snapshot finden Sie unter Tagging Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.

[RDS.30] RDS-DB-Instances sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBInstance`

AWS Config Regel: `tagged-rds-dbinstance` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon RDS-DB-Instance Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die DB-Instance keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die DB-Instance mit keinem Schlüssel gekennzeichnet ist. System-Tags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer RDS-DB-Instance finden Sie unter Tagging Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.

[RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBSecurityGroup`

AWS Config Regel: `tagged-rds-dbsecuritygroup` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon RDS-DB-Sicherheitsgruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind`requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die DB-Sicherheitsgruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die DB-Sicherheitsgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer RDS-DB-Sicherheitsgruppe finden Sie unter Tagging Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.

[RDS.32] RDS-DB-Snapshots sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBSnapshot`

AWS Config Regel: `tagged-rds-dbsnapshot` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon RDS-DB-Snapshot Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der DB-Snapshot keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der DB-Snapshot mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem RDS-DB-Snapshot finden Sie unter Tagging Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.

[RDS.33] RDS-DB-Subnetzgruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::RDS::DBSubnetGroup`

AWS Config Regel: `tagged-rds-dbsubnetgroups` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon RDS-DB-Subnetzgruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die DB-Subnetzgruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die DB-Subnetzgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien

für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer RDS-DB-Subnetzgruppe finden Sie unter Tagging Amazon RDS-Ressourcen im Amazon RDS-Benutzerhandbuch.

[RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.r5 AU-3 R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config Regel: **`rds-aurora-mysql-audit-logging-enabled`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob ein Amazon Aurora MySQL-DB-Cluster so konfiguriert ist, dass er Audit-Logs in Amazon CloudWatch Logs veröffentlicht. Die Steuerung schlägt fehl, wenn der Cluster nicht für die Veröffentlichung von Audit-Logs in Logs konfiguriert ist. CloudWatch

In Auditprotokollen werden Datenbankaktivitäten aufgezeichnet, darunter Anmeldeversuche, Datenänderungen, Schemaänderungen und andere Ereignisse, die aus Sicherheits- und Compliance-Gründen geprüft werden können. Wenn Sie einen Aurora MySQL-DB-Cluster so konfigurieren, dass er Audit-Logs in einer Protokollgruppe in Amazon CloudWatch Logs veröffentlicht, können Sie eine Echtzeitanalyse der Protokolldaten durchführen. CloudWatch Logs speichert Protokolle in einem äußerst langlebigen Speicher. Sie können auch Alarme erstellen und Messwerte in anzeigen CloudWatch.

> **Note**
>
> Eine alternative Möglichkeit, Audit-Logs in Logs zu CloudWatch veröffentlichen, besteht darin, die erweiterte Überwachung zu aktivieren und den DB-Parameter `server_audit_logs_upload` auf Clusterebene auf zu setzen. `1` Die Standardeinstellung für ist`server_audit_logs_upload parameter`. `0` Wir empfehlen jedoch, stattdessen die folgenden Anweisungen zur Problembehebung zu verwenden, um diese Kontrolle zu bestehen.

Abhilfe

Informationen zum Veröffentlichen von Aurora CloudWatch MySQL-DB-Cluster-Prüfprotokollen in Logs finden Sie unter Veröffentlichen von Amazon Aurora CloudWatch Aurora-MySQL-Protokollen in Amazon Logs im Amazon Aurora Aurora-Benutzerhandbuch.

[RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 SI-2, NIST.800-53.R5 SI-2 (2), NIST.800-53.R5 SI-2 (4), NIst.800-53.R5 SI-2 (5)

Kategorie: Erkennen > Sicherheitslücken-, Patch- und Versionsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::RDS::DBCluster`

AWS Config Regel: **`rds-cluster-auto-minor-version-upgrade-enable`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob das automatische Upgrade einer Nebenversion für einen Amazon RDS Multi-AZ-DB-Cluster aktiviert ist. Die Steuerung schlägt fehl, wenn das automatische Upgrade der Nebenversion für den Multi-AZ-DB-Cluster nicht aktiviert ist.

RDS bietet ein automatisches Upgrade der Nebenversion, sodass Sie Ihren Multi-AZ-DB-Cluster auf dem neuesten Stand halten können. Nebenversionen können neue Softwarefunktionen, Bugfixes, Sicherheitspatches und Leistungsverbesserungen einführen. Durch die Aktivierung des automatischen Upgrades für Nebenversionen auf RDS-Datenbankclustern erhält der Cluster zusammen mit den Instances im Cluster automatische Updates für die Nebenversion, sobald neue Versionen verfügbar sind. Die Updates werden während des Wartungsfensters automatisch angewendet.

Abhilfe

Informationen zur Aktivierung des automatischen Upgrades auf Multi-AZ-DB-Clustern finden Sie unter Ändern eines Multi-AZ-DB-Clusters im Amazon RDS-Benutzerhandbuch.

Amazon Redshift Redshift-Steuerelemente

Diese Kontrollen beziehen sich auf Amazon Redshift Redshift-Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.R5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.R5 AC-3. R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21)), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen, die nicht öffentlich zugänglich sind

Schweregrad: Kritisch

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: `redshift-cluster-public-access-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon Redshift Redshift-Cluster öffentlich zugänglich sind. Es wertet das `PubliclyAccessible` Feld im Cluster-Konfigurationselement aus.

Das `PubliclyAccessible` Attribut der Amazon Redshift Redshift-Cluster-Konfiguration gibt an, ob der Cluster öffentlich zugänglich ist. Wenn der Cluster mit „`PubliclyAccessible`gesetzt auf“ konfiguriert ist`true`, handelt es sich um eine mit dem Internet verbundene Instance mit einem öffentlich auflösbaren DNS-Namen, der in eine öffentliche IP-Adresse aufgelöst wird.

Wenn der Cluster nicht öffentlich zugänglich ist, handelt es sich um eine interne Instanz mit einem DNS-Namen, der in eine private IP-Adresse aufgelöst wird. Sofern Sie nicht beabsichtigen, dass Ihr Cluster öffentlich zugänglich ist, sollte der Cluster nicht mit der `PubliclyAccessible` Einstellung auf `true` konfiguriert werden.

Abhilfe

Informationen zum Aktualisieren eines Amazon Redshift-Clusters zur Deaktivierung des öffentlichen Zugriffs finden Sie unter Modifizieren eines Clusters im Amazon Redshift Management Guide. Stellen Sie Öffentlich zugänglich auf Nein ein.

[Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden

Verwandte Anforderungen: NIst.800-53.R5 AC-4, NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-23, NIST.800-53.R5 SC-23 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIst.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 R5 SC-8 (2)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten währen der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster` `AWS::Redshift::ClusterParameterGroup`

AWS Config -Regel: `redshift-require-tls-ssl`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Verbindungen zu Amazon Redshift Redshift-Clustern erforderlich sind, um Verschlüsselung bei der Übertragung zu verwenden. Die Prüfung schlägt fehl, wenn der Amazon Redshift Redshift-Clusterparameter `require_SSL` nicht auf `True` gesetzt ist.

TLS kann verwendet werden, um zu verhindern, dass potenzielle Angreifer person-in-the-middle oder ähnliche Angriffe verwenden, um den Netzwerkverkehr zu belauschen oder zu manipulieren. Nur verschlüsselte Verbindungen über TLS sollten zugelassen werden. Das Verschlüsseln von Daten während der Übertragung kann die Leistung beeinträchtigen. Sie sollten Ihre Anwendung mit dieser Funktion testen, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen.

Abhilfe

Informationen zum Aktualisieren einer Amazon Redshift-Parametergruppe, sodass eine Verschlüsselung erforderlich ist, finden Sie unter Ändern einer Parametergruppe im Amazon Redshift Management Guide. Auf True setzen**`require_ssl`**.

[Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6, NIST.800-53.R5 CP-6 (1), NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 CP-9, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-13 (5)

Kategorie: Wiederherstellen > Resilienz > Backups aktiviert

Schweregrad: Mittel

Ressourcentyp: `AWS::Redshift::Cluster`

AWS Config -Regel: `redshift-backup-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert	
`MinRetentionPeriod`	Minimale Aufbewahrungsdauer für Snapshots in Tagen	Ganzzahl	7 auf 35	7	

Dieses Steuerelement prüft, ob in einem Amazon Redshift Redshift-Cluster automatische Snapshots aktiviert sind und ob eine Aufbewahrungsdauer größer oder gleich dem angegebenen Zeitraum ist. Die Kontrolle schlägt fehl, wenn automatische Snapshots für den Cluster nicht aktiviert sind oder wenn die Aufbewahrungsdauer den angegebenen Zeitraum unterschreitet. Sofern Sie keinen benutzerdefinierten Parameterwert für die Aufbewahrungsdauer von Snapshots angeben, verwendet Security Hub einen Standardwert von 7 Tagen.

Mithilfe von Backups können Sie sich nach einem Sicherheitsvorfall schneller erholen. Sie stärken die Widerstandsfähigkeit Ihrer Systeme. Amazon Redshift erstellt standardmäßig regelmäßig Snapshots. Dieses Steuerelement prüft, ob automatische Snapshots aktiviert sind und mindestens sieben Tage lang aufbewahrt werden. Weitere Informationen zu automatisierten Amazon Redshift-Snapshots finden Sie unter Automatisierte Snapshots im Amazon Redshift Management Guide.

Abhilfe

Informationen zur Aktualisierung der Aufbewahrungsdauer von Snapshots für einen Amazon Redshift-Cluster finden Sie unter Modifizieren eines Clusters im Amazon Redshift Management Guide. Stellen Sie für Backup die Snapshot-Aufbewahrung auf einen Wert von 7 oder höher ein.

[Redshift.4] Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.r5 AU-3 R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config Regel: `redshift-cluster-audit-logging-enabled` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

- `loggingEnabled = true`(nicht anpassbar)

Dieses Steuerelement prüft, ob für einen Amazon Redshift Redshift-Cluster die Audit-Protokollierung aktiviert ist.

Die Amazon Redshift Redshift-Audit-Protokollierung bietet zusätzliche Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Cluster. Diese Daten können in Amazon S3 gespeichert und gesichert werden und können bei Sicherheitsüberprüfungen und Untersuchungen hilfreich sein. Weitere Informationen finden Sie unter Protokollierung von Datenbankprüfungen im Amazon Redshift Management Guide.

Abhilfe

Informationen zur Konfiguration der Audit-Protokollierung für einen Amazon Redshift-Cluster finden Sie unter Konfiguration der Überwachung mithilfe der Konsole im Amazon Redshift Management Guide.

[Redshift.6] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CP-9, NIst.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-2, NIst.800-53.R5 SI-2 (2), NIst.800-53.R5 SI-2 (4), Nist.800-53.R5 SI-2 (4) IST.800-53.r5 SI-2 (5)

Kategorie: Erkennen > Schwachstellen- und Patch-Management

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: `redshift-cluster-maintenancesettings-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `allowVersionUpgrade = true`(nicht anpassbar)

Dieses Steuerelement prüft, ob automatische Hauptversions-Upgrades für den Amazon Redshift Redshift-Cluster aktiviert sind.

Durch die Aktivierung automatischer Hauptversions-Upgrades wird sichergestellt, dass die neuesten Hauptversionsupdates für Amazon Redshift Redshift-Cluster während des Wartungsfensters installiert werden. Diese Updates können Sicherheitspatches und Bugfixes enthalten. Es ist ein wichtiger Schritt zur Sicherung von Systemen, über die Installation von Patches auf dem Laufenden zu bleiben.

Abhilfe

Um dieses Problem von zu beheben AWS CLI, verwenden Sie den Amazon Redshift `modify-cluster` Redshift-Befehl, um das `--allow-version-upgrade` Attribut festzulegen.

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

Wo *`clustername`* ist der Name Ihres Amazon Redshift Redshift-Clusters.

[Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden

Verwandte Anforderungen: NIst.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Privater API-Zugriff

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: `redshift-enhanced-vpc-routing-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster `EnhancedVpcRouting` aktiviert wurde.

Durch das verbesserte VPC-Routing wird der gesamte `COPY` `UNLOAD` Datenverkehr zwischen dem Cluster und den Datenrepositorys über Ihre VPC geleitet. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können VPC Flow Logs auch verwenden, um den Netzwerkverkehr zu überwachen.

Abhilfe

Detaillierte Anweisungen zur Problembehebung finden Sie unter Enabling enhanced VPC Routing im Amazon Redshift Management Guide.

[Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: `redshift-default-admin-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster den Standardwert des Admin-Benutzernamens geändert hat. Diese Steuerung schlägt fehl, wenn der Admin-Benutzername für einen Redshift-Cluster auf `awsuser` gesetzt ist.

Wenn Sie einen Redshift-Cluster erstellen, sollten Sie den standardmäßigen Administratorbenutzernamen in einen eindeutigen Wert ändern. Standardbenutzernamen sind allgemein bekannt und sollten bei der Konfiguration geändert werden. Durch das Ändern der Standardbenutzernamen wird das Risiko eines unbeabsichtigten Zugriffs verringert.

Abhilfe

Sie können den Admin-Benutzernamen für Ihren Amazon Redshift Redshift-Cluster nicht mehr ändern, nachdem er erstellt wurde. Um einen neuen Cluster zu erstellen, folgen Sie den Anweisungen hier.

[Redshift.9] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Identifizieren > Ressourcenkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: `redshift-default-db-name-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster den Datenbanknamen gegenüber seinem Standardwert geändert hat. Die Steuerung schlägt fehl, wenn der Datenbankname für einen Redshift-Cluster auf `dev` gesetzt ist.

Wenn Sie einen Redshift-Cluster erstellen, sollten Sie den Standarddatenbanknamen in einen eindeutigen Wert ändern. Standardnamen sind allgemein bekannt und sollten bei der Konfiguration geändert werden. Beispielsweise könnte ein bekannter Name zu unbeabsichtigtem Zugriff führen, wenn er in IAM-Richtlinienbedingungen verwendet wird.

Abhilfe

Sie können den Datenbanknamen für Ihren Amazon Redshift Redshift-Cluster nicht ändern, nachdem er erstellt wurde. Anweisungen zum Erstellen eines neuen Clusters finden Sie unter Erste Schritte mit Amazon Redshift im Amazon Redshift Getting Started Guide.

[Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Ressourcentyp: `AWS::Redshift::Cluster`

AWS Config -Regel: `redshift-cluster-kms-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob Amazon Redshift Redshift-Cluster im Ruhezustand verschlüsselt sind. Die Steuerung schlägt fehl, wenn ein Redshift-Cluster im Ruhezustand nicht verschlüsselt ist oder wenn sich der Verschlüsselungsschlüssel von dem im Regelparameter angegebenen Schlüssel unterscheidet.

In Amazon Redshift können Sie die Datenbankverschlüsselung für Ihre Cluster aktivieren, um Data-at-Rest besser zu schützen. Wenn Sie die Verschlüsselung für einen Cluster aktivieren, werden die Datenblöcke und die Metadaten des Systems für den Cluster und Snapshots des Clusters verschlüsselt. Die Verschlüsselung von Daten im Ruhezustand ist eine empfohlene bewährte Methode, da sie Ihren Daten eine Ebene der Zugriffsverwaltung hinzufügt. Durch die Verschlüsselung von Redshift-Clustern im Ruhezustand wird das Risiko verringert, dass ein nicht autorisierter Benutzer auf die auf der Festplatte gespeicherten Daten zugreifen kann.

Abhilfe

Informationen zur Änderung eines Redshift-Clusters für die Verwendung der KMS-Verschlüsselung finden Sie unter Ändern der Cluster-Verschlüsselung im Amazon Redshift Management Guide.

[Redshift.11] Redshift-Cluster sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config Regel: `tagged-redshift-cluster` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster Tags mit den spezifischen Schlüsseln hat, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Cluster keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel hat. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Cluster mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Redshift-Cluster finden Sie unter Tagging resources in Amazon Redshift im Amazon Redshift Management Guide.

[Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Redshift::EventSubscription`

AWS Config Regel: `tagged-redshift-eventsubscription` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster-Snapshot Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Cluster-Snapshot keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Cluster-Snapshot mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Abonnement für Redshift-Ereignisbenachrichtigungen finden Sie unter Tagging resources in Amazon Redshift im Amazon Redshift Management Guide.

[Redshift.13] Redshift-Cluster-Snapshots sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Redshift::ClusterSnapshot`

AWS Config Regel: `tagged-redshift-clustersnapshot` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein Amazon Redshift Redshift-Cluster-Snapshot Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn der Cluster-Snapshot keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Cluster-Snapshot mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von

Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Redshift-Cluster-Snapshot finden Sie unter Tagging resources in Amazon Redshift im Amazon Redshift Management Guide.

[Redshift.14] Redshift-Cluster-Subnetzgruppen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Redshift::ClusterSubnetGroup`

AWS Config Regel: `tagged-redshift-clustersubnetgroup` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource	StringList	Liste der Tags, die	`No default value`

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.		die AWS Anforderungen erfüllen	

Dieses Steuerelement prüft, ob eine Amazon Redshift Redshift-Cluster-Subnetzgruppe Tags mit den spezifischen Schlüsseln hat, die im Parameter definiert sind. `requiredTagKeys` Die Steuerung schlägt fehl, wenn die Cluster-Subnetzgruppe keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter angegebenen Schlüssel hat. `requiredTagKeys` Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Cluster-Subnetzgruppe mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter

AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Redshift-Cluster-Subnetzgruppe finden Sie unter Tagging resources in Amazon Redshift im Amazon Redshift Management Guide.

[Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Konfiguration von Sicherheitsgruppen

Schweregrad: Hoch

Art der Ressource: `AWS::Redshift::Cluster`

AWS Config -Regel: `redshift-unrestricted-port-access`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob eine mit einem Amazon Redshift Redshift-Cluster verknüpfte Sicherheitsgruppe über Eingangsregeln verfügt, die den Zugriff auf den Cluster-Port vom Internet aus ermöglichen (0.0.0.0/0 oder: :/0). Die Kontrolle schlägt fehl, wenn die Eingangsregeln der Sicherheitsgruppe den Zugriff auf den Cluster-Port über das Internet zulassen.

Die Zulassung eines uneingeschränkten eingehenden Zugriffs auf den Redshift-Cluster-Port (IP-Adresse mit dem Suffix /0) kann zu unbefugtem Zugriff oder Sicherheitsvorfällen führen. Wir empfehlen, bei der Erstellung von Sicherheitsgruppen und der Konfiguration von Regeln für eingehenden Datenverkehr das Prinzip des Zugriffs mit den geringsten Rechten anzuwenden.

Abhilfe

Informationen zur Beschränkung des Eingangs auf dem Redshift-Cluster-Port auf eingeschränkte Ursprünge finden Sie unter Arbeiten mit Sicherheitsgruppenregeln im Amazon VPC-Benutzerhandbuch. Aktualisieren Sie Regeln, bei denen der Portbereich mit dem Redshift-Cluster-Port übereinstimmt und der IP-Portbereich 0.0.0.0/0 ist.

Amazon Route 53-Steuerelemente

Diese Kontrollen beziehen sich auf Route 53-Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Route53::HealthCheck`

AWS Config Regel: `tagged-route53-healthcheck` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon Route 53-Zustandsprüfung Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die Zustandsprüfung keine Tag-Schlüssel enthält oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl,

wenn die Zustandsprüfung mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Stichwörtern zu einer Route 53-Zustandsprüfung finden Sie unter Benennen und Kennzeichnen von Zustandsprüfungen im Amazon Route 53-Entwicklerhandbuch.

[Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.r5 AU-3 R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::Route53::HostedZone`

AWS Config -Regel: `route53-query-logging-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die DNS-Abfrageprotokollierung für eine öffentlich gehostete Zone von Amazon Route 53 aktiviert ist. Die Steuerung schlägt fehl, wenn die DNS-Abfrageprotokollierung für eine öffentlich gehostete Route 53-Zone nicht aktiviert ist.

Das Protokollieren von DNS-Abfragen für eine von Route 53 gehostete Zone entspricht den DNS-Sicherheits- und Compliance-Anforderungen und sorgt für Transparenz. Die Protokolle enthalten Informationen wie die abgefragte Domäne oder Subdomäne, Datum und Uhrzeit der Abfrage, den DNS-Eintragstyp (z. B. A oder AAAA) und den DNS-Antwortcode (z. B. oder). `NoError` `ServFail` Wenn die DNS-Abfrageprotokollierung aktiviert ist, veröffentlicht Route 53 die Protokolldateien in Amazon CloudWatch Logs.

Abhilfe

Informationen zum Protokollieren von DNS-Abfragen für öffentlich gehostete Route 53-Zonen finden Sie unter Konfiguration der Protokollierung für DNS-Abfragen im Amazon Route 53-Entwicklerhandbuch.

Steuerelemente von Amazon Simple Storage Service

Diese Kontrollen beziehen sich auf Amazon S3 S3-Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein

> **Important**
>
> Am 12. März 2024 wurde der Titel dieses Steuerelements in den angezeigten Titel geändert. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/2.1.4, AWS CIS Foundations Benchmark v1.4.0/2.1.5, PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-2, Nist.800-53.r5 AC-3, Nist.800-53.r5 NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SNIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9))

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config -Regel: `s3-account-level-public-access-blocks-periodic`

Art des Zeitplans: Periodisch

Parameter:

- `ignorePublicAcls`: `true` (nicht anpassbar)
- `blockPublicPolicy`: `true` (nicht anpassbar)
- `blockPublicAcls`: `true` (nicht anpassbar)
- `restrictPublicBuckets`: `true` (nicht anpassbar)

Diese Kontrolle prüft, ob die oben genannten Amazon S3 S3-Einstellungen für den öffentlichen Zugriff blockieren auf Kontoebene für einen S3-Allzweck-Bucket konfiguriert sind. Die Steuerung schlägt fehl, wenn eine oder mehrere der Einstellungen zum Blockieren des öffentlichen Zugriffs auf gesetzt sind`false`.

Die Steuerung schlägt fehl`false`, wenn eine der Einstellungen auf eingestellt ist oder wenn eine der Einstellungen nicht konfiguriert ist.

Amazon S3 Public Access Block wurde entwickelt, um Kontrollen auf der gesamten AWS-Konto oder auf der Ebene einzelner S3-Buckets bereitzustellen, um sicherzustellen, dass Objekte niemals öffentlich zugänglich sind. Öffentlicher Zugriff auf Buckets und Objekte wird über Zugriffskontrolllisten (ACLs), Bucket-Richtlinien oder beides gewährt.

Sofern Sie nicht beabsichtigen, Ihre S3-Buckets öffentlich zugänglich zu machen, sollten Sie die Amazon S3 Block Public Access-Funktion auf Kontoebene konfigurieren.

Weitere Informationen finden Sie unter Verwenden von Amazon S3 Block Public Access im Amazon Simple Storage Service-Benutzerhandbuch.

Abhilfe

Informationen zur Aktivierung von Amazon S3 Block Public Access für Sie AWS-Konto finden Sie unter Konfiguration der Einstellungen für den Block Public Access für Ihr Konto im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.2] S3-Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren

> **Important**
>
> Am 12. März 2024 wurde der Titel dieses Steuerelements in den angezeigten Titel geändert. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.R5 AC-21, NIST.800-53.r5 AC-3, NIst.800-53.r5 AC-3 (7), NIST.800-53.R5 AC-3 R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21)), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: `s3-bucket-public-read-prohibited`

Art des Zeitplans: Periodisch und durch Änderung ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket öffentlichen Lesezugriff gewährt. Es überprüft die Einstellungen für „Block Public Access“ (Blockieren des öffentlichen Zugriffs), die

Bucket-Richtlinie und die Bucket-Zugriffskontrollliste (ACL). Die Kontrolle schlägt fehl, wenn der Bucket öffentlichen Lesezugriff gewährt.

In einigen Anwendungsfällen kann es erforderlich sein, dass jeder im Internet aus Ihrem S3-Bucket lesen kann. Solche Situationen sind jedoch selten. Um die Integrität und Sicherheit Ihrer Daten zu gewährleisten, sollte Ihr S3-Bucket nicht öffentlich lesbar sein.

Abhilfe

Informationen zum Blockieren des öffentlichen Lesezugriffs auf Ihre Amazon S3 S3-Buckets finden Sie unter Konfiguration der Einstellungen zum Sperren des öffentlichen Zugriffs für Ihre S3-Buckets im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren

> **Important**
>
> Am 12. März 2024 wurde der Titel dieses Steuerelements in den angezeigten Titel geändert. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20) NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Kritisch

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: `s3-bucket-public-write-prohibited`

Art des Zeitplans: Periodisch und durch Änderung ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket öffentlichen Schreibzugriff zulässt. Es überprüft die Einstellungen für „Block Public Access“ (Blockieren des öffentlichen Zugriffs), die Bucket-Richtlinie und die Bucket-Zugriffskontrollliste (ACL). Die Kontrolle schlägt fehl, wenn der Bucket öffentlichen Schreibzugriff zulässt.

Einige Anwendungsfälle erfordern, dass jeder im Internet in den S3-Bucket schreiben kann. Solche Situationen sind jedoch selten. Um die Integrität und Sicherheit Ihrer Daten zu gewährleisten, sollte Ihr S3-Bucket nicht öffentlich beschreibbar sein.

Abhilfe

Informationen zum Blockieren des öffentlichen Schreibzugriffs auf Ihre Amazon S3 S3-Buckets finden Sie unter Konfiguration der Einstellungen zum Sperren des öffentlichen Zugriffs für Ihre S3-Buckets im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern

> **Important**
>
> Am 12. März 2024 wurde der Titel dieses Steuerelements in den angezeigten Titel geändert. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/2.1.1, CIS AWS Foundations Benchmark v1.4.0/2.1.2, PCI DSS v3.2.1/4.1, NIST.800-53.R5 AC-17 (2), NIST.800-53.R5 AC-4, NIST.800-53.R5 IA-5 (1), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-23, NIST.800-53.R5 SC-23 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-8 (1), NIST.800-53.R5 SC-8 (2), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: `s3-bucket-ssl-requests-only`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket über eine Richtlinie verfügt, nach der Anfragen SSL verwenden müssen. Die Kontrolle schlägt fehl, wenn die Bucket-Richtlinie keine Anfragen zur Verwendung von SSL erfordert.

S3-Buckets sollten über Richtlinien verfügen, die vorschreiben, dass alle Anfragen (`Action: S3:*`) in der S3-Ressourcenrichtlinie, wie durch den Bedingungsschlüssel `aws:SecureTransport` angegeben, nur die Übertragung von Daten über HTTPS akzeptieren.

Abhilfe

Informationen zur Aktualisierung einer Amazon S3 S3-Bucket-Richtlinie, um unsicheren Transport zu verweigern, finden Sie unter Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole im Amazon Simple Storage Service-Benutzerhandbuch.

Fügen Sie eine Richtlinienerklärung hinzu, die der in der folgenden Richtlinie ähnelt. `DOC-EXAMPLE-BUCKET`Ersetzen Sie es durch den Namen des Buckets, den Sie ändern.

```
{
    "Id": "ExamplePolicy",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ],
            "Condition": {
                "Bool": {
                     "aws:SecureTransport": "false"
                }
            },
           "Principal": "*"
        }
    ]
}
```

Weitere Informationen finden Sie unter Welche S3-Bucket-Richtlinie sollte ich verwenden, um die AWS Config Regel s3- einzuhaltenbucket-ssl-requests-only? im AWS offiziellen Knowledge Center.

[S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten

> **Important**
>
> Am 12. März 2024 wurde der Titel dieses Steuerelements in den angezeigten Titel geändert. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schützen > Sichere Zugriffsverwaltung > Eingeschränkte Aktionen für sensible API-Operationen

Schweregrad: Hoch

Art der Ressource: `AWS::S3::Bucket`

AWS Config-Regel: `s3-bucket-blacklisted-actions-prohibited`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `blacklistedactionpatterns`: `s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl` (nicht anpassbar)

Diese Kontrolle prüft, ob eine allgemeine Amazon S3 S3-Bucket-Richtlinie verhindert, dass Principals AWS-Konten von anderen Personen verweigerte Aktionen für Ressourcen im S3-Bucket ausführen. Die Kontrolle schlägt fehl, wenn die Bucket-Richtlinie eine oder mehrere der vorherigen Aktionen für einen Prinzipal in einem anderen AWS-Konto zulässt.

Die Implementierung des Zugriffs mit den geringsten Rechten ist von grundlegender Bedeutung, um das Sicherheitsrisiko und die Auswirkungen von Fehlern oder böswilligen Absichten zu verringern. Wenn eine S3-Bucket-Richtlinie den Zugriff von externen Konten aus ermöglicht, kann dies zu einer Datenexfiltration durch eine Insider-Bedrohung oder einen Angreifer führen.

Der `blacklistedactionpatterns` Parameter ermöglicht eine erfolgreiche Auswertung der Regel für S3-Buckets. Der Parameter gewährt Zugriff auf externe Konten für Aktionsmuster, die nicht in der `blacklistedactionpatterns` Liste enthalten sind.

Abhilfe

Informationen zum Aktualisieren einer Amazon S3 S3-Bucket-Richtlinie zum Entfernen von Berechtigungen finden Sie unter. Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole im Amazon Simple Storage Service-Benutzerhandbuch.

Führen Sie auf der Seite Bucket-Richtlinie bearbeiten im Textfeld zur Richtlinienbearbeitung eine der folgenden Aktionen aus:

- Entfernen Sie die Anweisungen, die anderen AWS-Konten Zugriff auf verweigerte Aktionen gewähren.
- Entfernen Sie die zulässigen verweigerten Aktionen aus den Anweisungen.

[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden

> **Important**
>
> Am 12. März 2024 wurde der Titel dieses Steuerelements in den abgebildeten Titel geändert. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: PCI DSS v3.2.1/2.2, NIST.800-53.R5 AU-9 (2), NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6, NIst.800-53.R5 CP-6 (1), NIST.800-53.R5 CP-6 (2), NIst.800-53.r5 CP-9, NIst.800-53.R5 SC-36 (2), NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Niedrig

Art der Ressource: `AWS::S3::Bucket`

AWS Config Regel: **`s3-bucket-cross-region-replication-enabled`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen Amazon S3 S3-Allzweck-Bucket die regionsübergreifende Replikation aktiviert ist. Die Steuerung schlägt fehl, wenn für den Bucket keine regionsübergreifende Replikation aktiviert ist.

Bei der Replikation handelt es sich um das automatische, asynchrone Kopieren von Objekten zwischen Buckets desselben oder eines anderen. AWS-Regionen Bei der Replikation werden neu erstellte Objekte und Objektaktualisierungen von einem Quell-Bucket in einen oder mehrere Ziel-Buckets kopiert. AWS In bewährten Verfahren wird die Replikation für Quell- und Ziel-Buckets empfohlen, die demselben Eigentümer gehören. AWS-Konto Zusätzlich zur Verfügbarkeit sollten Sie andere Einstellungen für die Systemstabilisierung berücksichtigen.

Abhilfe

Informationen zur Aktivierung der regionsübergreifenden Replikation auf einem S3-Bucket finden Sie unter Konfiguration der Replikation für Quell- und Ziel-Buckets, die demselben Konto gehören, im Amazon Simple Storage Service-Benutzerhandbuch. Wählen Sie für Quell-Bucket die Option Auf alle Objekte im Bucket anwenden aus.

[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/2.1.4, CIS AWS Foundations Benchmark v1.4.0/2.1.5, NIst.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-4, NIst.800-53.r5 AC-6, NISt.800-53.r5 AC-6, NISt.NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (4), Nist.800-53.R5 SC-7 (4) IST.800-53.r5 SC-7 (9)

Kategorie: Schützen > Sicheres Zugriffsmanagement > Zugriffskontrolle

Schweregrad: Hoch

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: `s3-bucket-level-public-access-prohibited`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

- `excludedPublicBuckets`(nicht anpassbar) — Eine durch Kommas getrennte Liste bekannter zulässiger öffentlicher S3-Bucket-Namen

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket den öffentlichen Zugriff auf Bucket-Ebene blockiert. Die Steuerung schlägt fehl, wenn eine der folgenden Einstellungen auf gesetzt ist`false`:

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`
- `restrictPublicBuckets`

Block Public Access auf S3-Bucket-Ebene bietet Kontrollen, mit denen sichergestellt wird, dass Objekte niemals öffentlich zugänglich sind. Öffentlicher Zugriff auf Buckets und Objekte wird über Zugriffskontrolllisten (ACLs), Bucket-Richtlinien oder beides gewährt.

Sofern Sie nicht beabsichtigen, Ihre S3-Buckets öffentlich zugänglich zu machen, sollten Sie die Amazon S3 Block Public Access-Funktion auf Bucket-Ebene konfigurieren.

Abhilfe

Informationen zum Entfernen des öffentlichen Zugriffs auf Bucket-Ebene finden Sie unter Blockieren des öffentlichen Zugriffs auf Ihren Amazon S3 S3-Speicher im Amazon S3 S3-Benutzerhandbuch.

[S3.9] Bei S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein

> **Important**
>
> Am 12. März 2024 wurde der Titel dieses Steuerelements in den angezeigten Titel geändert. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (4), NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AC-6 (9), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.r5 AU-3 R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: `s3-bucket-logging-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Serverzugriffsprotokollierung für einen Amazon S3 S3-Allzweck-Bucket aktiviert ist. Die Steuerung schlägt fehl, wenn die Serverzugriffsprotokollierung nicht aktiviert ist. Wenn die Protokollierung aktiviert ist, übermittelt Amazon S3 Zugriffsprotokolle für einen Quell-Bucket an einen ausgewählten Ziel-Bucket. Der Ziel-Bucket muss sich im selben AWS-Region wie der Quell-Bucket befinden und es darf kein standardmäßiger Aufbewahrungszeitraum konfiguriert sein. Für den Ziel-Logging-Bucket muss die Serverzugriffsprotokollierung nicht aktiviert sein, und Sie sollten die Ergebnisse für diesen Bucket unterdrücken.

Die Serverzugriffsprotokollierung bietet detaillierte Aufzeichnungen der Anfragen, die an einen Bucket gestellt wurden. Serverzugriffsprotokolle können bei Sicherheits- und Zugriffsprüfungen hilfreich sein. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon S3: Aktivieren Sie die Amazon S3 S3-Serverzugriffsprotokollierung.

Abhilfe

Informationen zur Aktivierung der Amazon S3 S3-Serverzugriffsprotokollierung finden Sie unter Aktivieren der Amazon S3 S3-Serverzugriffsprotokollierung im Amazon S3 S3-Benutzerhandbuch.

[S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben

> **Important**
>
> Am 12. März 2024 wurde der Titel dieses Steuerelements in den angezeigten Titel geändert. Security Hub hat diese Kontrolle im April 2024 aus dem Standard AWS Foundational Security Best Practices entfernt, sie ist jedoch weiterhin im Standard NIST SP 800-53 Rev. 5 enthalten. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 CP-9, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: `s3-version-lifecycle-policy-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein versionsbasierter Amazon S3 S3-Bucket für allgemeine Zwecke über eine Lifecycle-Konfiguration verfügt. Die Kontrolle schlägt fehl, wenn der Bucket keine Lifecycle-Konfiguration hat.

Wir empfehlen, eine Lifecycle-Konfiguration für Ihren S3-Bucket zu erstellen, um Ihnen bei der Definition von Aktionen zu helfen, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll.

Abhilfe

Weitere Informationen zur Konfiguration des Lebenszyklus in einem Amazon S3 S3-Bucket finden Sie unter Lebenszykluskonfiguration für einen Bucket einrichten und Ihren Speicherlebenszyklus verwalten.

[S3.11] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein

> **Important**
>
> Am 12. März 2024 wurde der Titel dieses Steuerelements in den angezeigten Titel geändert. Security Hub hat dieses Steuerelement im April 2024 aus dem Standard AWS Foundational Security Best Practices entfernt, aber es ist immer noch im Standard NIST SP 800-53 Rev. 5 enthalten:. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4, NIST.800-53.R5 SI-4 (4)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: `s3-event-notifications-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`eventTypes`	Liste der bevorzugten S3-Ereignistypen	EnumList (maximal 28 Artikel)	`s3:IntelligentTiering`, `s3:LifecycleExpiration:*`, `s3:LifecycleExpiration:Delete`, `s3:LifecycleExpiration:DeleteMarkerCreated`, `s3:LifecycleTransition`, `s3:ObjectAcl:Put`, `s3:ObjectCreated:*`, `s3:ObjectCreated:C`	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
			ompleteMultipartUpload, s3:ObjectCreated:Copy, s3:ObjectCreated:Post, s3:ObjectCreated:Put, s3:ObjectRemoved:*, s3:ObjectRemoved:Delete, s3:ObjectRemoved:DeleteMarkerCreated, s3:ObjectRestore:*, s3:ObjectRestore:Completed, s3:ObjectRestore:Delete,	

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
			s3:ObjectRestore:Post, s3:ObjectTagging:*, s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplication, s3:Replication:OperationMissedThreshold, s3:Replication:OperationNotTracked,	

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
			`s3:Replication:OperationReplicatedAfterThreshold`, `s3:TestEvent`	

Dieses Steuerelement prüft, ob S3-Ereignisbenachrichtigungen in einem Amazon S3 S3-Allzweck-Bucket aktiviert sind. Die Steuerung schlägt fehl, wenn S3-Ereignisbenachrichtigungen für den Bucket nicht aktiviert sind. Wenn Sie benutzerdefinierte Werte für den `eventTypes` Parameter angeben, wird die Steuerung nur erfolgreich ausgeführt, wenn Ereignisbenachrichtigungen für die angegebenen Ereignistypen aktiviert sind.

Wenn Sie S3-Ereignisbenachrichtigungen aktivieren, erhalten Sie Benachrichtigungen, wenn bestimmte Ereignisse eintreten, die sich auf Ihre S3-Buckets auswirken. Sie können beispielsweise über die Erstellung, Entfernung von Objekten und Wiederherstellung von Objekten informiert werden. Diese Benachrichtigungen können die zuständigen Teams vor versehentlichen oder vorsätzlichen Änderungen warnen, die zu unberechtigtem Datenzugriff führen können.

Abhilfe

Informationen zum Erkennen von Änderungen an S3-Buckets und Objekten finden Sie unter Amazon S3 S3-Ereignisbenachrichtigungen im Amazon S3 S3-Benutzerhandbuch.

[S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten

> **Important**
>
> Am 12. März 2024 wurde der Titel dieses Steuerelements in den angezeigten Titel geändert. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-6

Kategorie: Schützen > Sichere Zugriffsverwaltung > Zugriffskontrolle

Schweregrad: Mittel

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: `s3-bucket-acl-prohibited`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket Benutzerberechtigungen mit einer Zugriffskontrollliste (ACL) bereitstellt. Die Kontrolle schlägt fehl, wenn eine ACL für die Verwaltung des Benutzerzugriffs auf den Bucket konfiguriert ist.

ACLs sind veraltete Zugriffskontrollmechanismen, die älter als IAM sind. Anstelle von ACLs empfehlen wir, S3-Bucket-Richtlinien oder AWS Identity and Access Management (IAM-) Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets zu verwalten.

Abhilfe

Um diese Kontrolle zu umgehen, sollten Sie ACLs für Ihre S3-Buckets deaktivieren. Anweisungen finden Sie unter Kontrolle des Besitzes von Objekten und Deaktivieren von ACLs für Ihren Bucket im Amazon Simple Storage Service-Benutzerhandbuch.

Informationen zum Erstellen einer S3-Bucket-Richtlinie finden Sie unter Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole. Informationen zum Erstellen einer IAM-

Benutzerrichtlinie für einen S3-Bucket finden Sie unter Steuern des Zugriffs auf einen Bucket mit Benutzerrichtlinien.

[S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben

> **Important**
>
> Am 12. März 2024 wurde der Titel dieses Steuerelements in den angezeigten Titel geändert. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 CP-9, NIST.800-53.R5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Kategorie: Schützen > Datenschutz

Schweregrad: Niedrig

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: `s3-lifecycle-policy-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`targetTransitionDays`	Anzahl der Tage nach der Objekterstellung, an denen Objekte in eine angegebene Speicherklasse umgestellt werden	Ganzzahl	`1` auf `36500`	Kein Standardwert
`targetExpirationDays`	Anzahl der Tage nach der Objekterstellung, an denen Objekte gelöscht werden	Ganzzahl	`1` auf `36500`	Kein Standardwert

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`targetTransitionStorageClass`	Typ der S3-Speicherklasse des Ziels	Enum	`STANDARD_IA`, `INTELLIGENT_TIERING`, `ONEZONE_IA`, `GLACIER`, `GLACIER_IR`, `DEEP_ARCHIVE`	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon S3 S3-Allzweck-Bucket über eine Lifecycle-Konfiguration verfügt. Die Steuerung schlägt fehl, wenn der Bucket keine Lifecycle-Konfiguration hat. Wenn Sie benutzerdefinierte Werte für einen oder mehrere der oben genannten Parameter angeben, ist die Kontrolle nur erfolgreich, wenn die Richtlinie die angegebene Speicherklasse, Löschzeit oder Übergangszeit beinhaltet.

Durch das Erstellen einer Lifecycle-Konfiguration für Ihren S3-Bucket werden Aktionen definiert, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll. Sie können beispielsweise Objekte in eine andere Speicherklasse übertragen, archivieren oder nach einem bestimmten Zeitraum löschen.

Abhilfe

Informationen zur Konfiguration von Lebenszyklusrichtlinien für einen Amazon S3 S3-Bucket finden Sie unter Einstellung der Lebenszykluskonfiguration für einen Bucket und unter Verwaltung Ihres Speicherlebenszyklus im Amazon S3 S3-Benutzerhandbuch.

[S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein

> **Important**
>
> Am 12. März 2024 wurde der Titel dieses Steuerelements in den angezeigten Titel geändert. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Verwandte Anforderungen: NIST.800-53.R5 AU-9 (2), NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-6, NIST.800-53.R5 CP-6 (1), NIST.800-53.R5 CP-6 (2), NIST.800-53.R5 CP-9, NIST.800-53.R5 SC-5 (2), NIST.800-53,R5 SI-12, NIST.800-53,R5 SI-13 (5)

Schweregrad: Niedrig

Art der Ressource: `AWS::S3::Bucket`

AWS Config -Regel: `s3-bucket-versioning-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für einen Amazon S3 S3-Allzweck-Bucket die Versionierung aktiviert ist. Die Kontrolle schlägt fehl, wenn die Versionierung für den Bucket ausgesetzt ist.

Bei der Versionierung werden mehrere Varianten eines Objekts im selben S3-Bucket aufbewahrt. Sie können die Versionierung verwenden, um frühere Versionen eines in Ihrem S3-Bucket gespeicherten Objekts beizubehalten, abzurufen und wiederherzustellen. Die Versionierung hilft Ihnen bei der Wiederherstellung sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsausfällen.

> **Tip**
>
> Wenn die Anzahl der Objekte in einem Bucket aufgrund der Versionierung zunimmt, können Sie eine Lifecycle-Konfiguration einrichten, um versionierte Objekte auf der Grundlage von Regeln automatisch zu archivieren oder zu löschen. Weitere Informationen finden Sie unter Amazon S3 Lifecycle Management für versionierte Objekte.

Abhilfe

Informationen zur Verwendung der Versionierung in einem S3-Bucket finden Sie unter Aktivieren der Versionierung für Buckets im Amazon S3 S3-Benutzerhandbuch.

[S3.15] Bei S3-Allzweck-Buckets sollte Object Lock aktiviert sein

> **Important**
>
> Am 12. März 2024 wurde der Titel dieses Steuerelements in den angezeigten Titel geändert. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Verwandte Anforderungen: NIST.800-53.R5 CP-6 (2)

Schweregrad: Mittel

Art der Ressource: `AWS::S3::Bucket`

AWS Config Regel: **`s3-bucket-default-lock-enabled`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`mode`	Aufbewahrungsmodus von S3 Object Lock	Enum	`GOVERNANCE`, `COMPLIANCE`	Kein Standardwert

Dieses Steuerelement prüft, ob in einem Amazon S3 S3-Allzweck-Bucket Object Lock aktiviert ist. Die Steuerung schlägt fehl, wenn Object Lock für den Bucket nicht aktiviert ist. Wenn Sie einen

benutzerdefinierten Wert für den `mode` Parameter angeben, wird die Steuerung nur erfolgreich ausgeführt, wenn S3 Object Lock den angegebenen Aufbewahrungsmodus verwendet.

Sie können S3 Object Lock verwenden, um Objekte mithilfe eines write-once-read-many (WORM-) Modells zu speichern. Object Lock kann verhindern, dass Objekte in S3-Buckets für einen bestimmten Zeitraum oder auf unbestimmte Zeit gelöscht oder überschrieben werden. Sie können die S3-Objektsperre verwenden, um regulatorische Anforderungen einzuhalten, die die WORM-Speicherung verlangen, oder um eine zusätzliche Schutzebene gegen Objektänderungen und -löschungen einzurichten.

Abhilfe

Informationen zur Konfiguration von Object Lock für neue und bestehende S3-Buckets finden Sie unter Konfiguration von S3 Object Lock im Amazon S3 S3-Benutzerhandbuch.

[S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys

> **Important**
>
> Am 12. März 2024 wurde der Titel dieses Steuerelements in den angezeigten Titel geändert. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Verwandte Anforderungen: NIST.800-53.R5 SC-12 (2), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 SI-7 (6), NIST.800-53.R5 AU-9

Schweregrad: Mittel

Art der Ressource: `AWS::S3::Bucket`

AWS Config Regel: **`s3-default-encryption-kms`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob ein Amazon S3 S3-Allzweck-Bucket mit einem AWS KMS key (SSE-KMS oder DSSE-KMS) verschlüsselt ist. Die Steuerung schlägt fehl, wenn der Bucket mit der Standardverschlüsselung (SSE-S3) verschlüsselt ist.

Serverseitige Verschlüsselung (SSE) ist die Verschlüsselung von Daten am Zielort durch die Anwendung oder den Dienst, der sie empfängt. Sofern Sie nichts anderes angeben, verwenden S3-Buckets standardmäßig Amazon S3 S3-verwaltete Schlüssel (SSE-S3) für die serverseitige Verschlüsselung. Für zusätzliche Kontrolle können Sie Buckets jedoch so konfigurieren, dass sie stattdessen serverseitige Verschlüsselung mit AWS KMS keys (SSE-KMS oder DSSE-KMS) verwenden. Amazon S3 verschlüsselt Ihre Daten auf Objektebene, wenn es sie auf Festplatten in AWS Rechenzentren schreibt, und entschlüsselt sie für Sie, wenn Sie darauf zugreifen.

Abhilfe

Informationen zum Verschlüsseln eines S3-Buckets mit SSE-KMS finden Sie unter Serverseitige Verschlüsselung mit AWS KMS (SSE-KMS) angeben im Amazon S3 S3-Benutzerhandbuch. Informationen zum Verschlüsseln eines S3-Buckets mit DSSE-KMS finden Sie unter Spezifizierung der serverseitigen Dual-Layer-Verschlüsselung mit AWS KMS keys (DSSE-KMS) im Amazon S3 S3-Benutzerhandbuch.

[S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schützen > Sicheres Zugriffsmanagement > Ressource nicht öffentlich zugänglich

Schweregrad: Kritisch

Art der Ressource: `AWS::S3::AccessPoint`

AWS Config Regel: **`s3-access-point-public-access-blocks`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Kontrolle prüft, ob für einen Amazon S3 S3-Zugriffspunkt die Einstellungen für den öffentlichen Zugriff blockiert aktiviert sind. Die Kontrolle schlägt fehl, wenn die Einstellungen zum Blockieren des öffentlichen Zugriffs für den Access Point nicht aktiviert sind.

Die Amazon S3 S3-Funktion Block Public Access hilft Ihnen, den Zugriff auf Ihre S3-Ressourcen auf drei Ebenen zu verwalten: auf Konto-, Bucket- und Zugriffspunktebene. Die Einstellungen auf jeder Ebene können unabhängig voneinander konfiguriert werden, sodass Sie unterschiedliche Stufen der öffentlichen Zugriffsbeschränkungen für Ihre Daten festlegen können. Die Einstellungen des Access Points können die restriktiveren Einstellungen auf höheren Ebenen (Kontoebene oder dem Access Point zugewiesener Bucket) nicht einzeln außer Kraft setzen. Stattdessen sind die Einstellungen auf der Zugriffspunktebene additiv, was bedeutet, dass sie die Einstellungen auf den anderen Ebenen ergänzen und mit ihnen zusammenarbeiten. Sofern Sie nicht beabsichtigen, dass ein S3-Zugriffspunkt öffentlich zugänglich ist, sollten Sie die Einstellungen zum Blockieren des öffentlichen Zugriffs aktivieren.

Abhilfe

Amazon S3 unterstützt derzeit nicht das Ändern der Public Block Access-Einstellungen eines Zugriffspunkts, nachdem der Zugriffspunkt erstellt wurde. Alle Einstellungen zum Blockieren des öffentlichen Zugriffs sind standardmäßig aktiviert, wenn Sie einen neuen Access Point erstellen. Wir empfehlen, alle Einstellungen aktiviert zu lassen, es sei denn, Sie wissen, dass Sie eine bestimmte Einstellung deaktivieren müssen. Weitere Informationen finden Sie unter Verwaltung des öffentlichen Zugriffs auf Access Points im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.20] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein

Verwandte Anforderungen: CIS AWS Foundations Benchmark v3.0.0/2.1.2, CIS AWS Foundations Benchmark v1.4.0/2.1.3, NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2, NIST.800-53.R5 CM-2 (2), NIST.800-53.R5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategorie: Schützen > Datenschutz > Schutz vor Datenlöschung

Schweregrad: Niedrig

Art der Ressource: `AWS::S3::Bucket`

AWS Config Regel: **`s3-bucket-mfa-delete-enabled`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob das Löschen mit Multi-Faktor-Authentifizierung (MFA) in einem Amazon S3 S3-Bucket mit allgemeiner Version aktiviert ist. Die Steuerung schlägt fehl, wenn MFA Delete für den Bucket nicht aktiviert ist. Das Steuerelement liefert keine Ergebnisse für Buckets mit einer Lifecycle-Konfiguration.

Wenn Sie mit der S3-Versionierung in Amazon S3 S3-Buckets arbeiten, können Sie optional eine weitere Sicherheitsebene hinzufügen, indem Sie einen Bucket so konfigurieren, dass er das MFA-Löschen aktiviert. In diesem Fall muss der Bucket-Eigentümer zwei Authentifizierungsformen in jede Anforderung aufnehmen, um eine Version zu löschen oder den Versioning-Status des Buckets zu ändern. MFA Delete bietet zusätzliche Sicherheit, falls Ihre Sicherheitsanmeldedaten gefährdet sind. Das Löschen mit MFA kann auch dazu beitragen, versehentliches Löschen von Buckets zu verhindern, indem der Benutzer, der die Löschaktion initiiert, den physischen Besitz eines MFA-Geräts mit einem MFA-Code nachweisen muss. Dadurch wird der Löschvorgang noch reibungsloser und sicherer.

> **Note**
>
> Die Funktion zum Löschen von MFA erfordert die Bucket-Versionierung als Abhängigkeit. Die Bucket-Versionierung ist eine Methode, mit der mehrere Varianten eines S3-Objekts im selben Bucket gespeichert werden. Darüber hinaus kann nur der Bucket-Besitzer, der als Root-Benutzer angemeldet ist, das Löschen von MFA aktivieren und Löschaktionen für S3-Buckets ausführen.

Abhilfe

Informationen zum Aktivieren der S3-Versionierung und zum Konfigurieren des MFA-Löschvorgangs für einen Bucket finden Sie unter Konfiguration des MFA-Löschvorgangs im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.22] S3-Allzweck-Buckets sollten Schreibereignisse auf Objektebene protokollieren

Verwandte Anforderungen: CIS Foundations Benchmark v3.0.0/3.8 AWS

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config Regel: **`cloudtrail-all-write-s3-data-event-check`**

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS-Konto über mindestens einen AWS CloudTrail Multiregions-Trail verfügt, der alle Schreibdatenereignisse für Amazon S3 S3-Buckets protokolliert. Die Kontrolle schlägt fehl, wenn das Konto nicht über einen Multi-Regions-Trail verfügt, der Schreibdatenereignisse für S3-Buckets protokolliert.

S3-Operationen auf Objektebene, wie, und `GetObject` `DeleteObject``PutObject`, werden als Datenereignisse bezeichnet. Standardmäßig protokolliert CloudTrail es keine Datenereignisse, aber Sie können Trails konfigurieren, um Datenereignisse für S3-Buckets zu protokollieren. Wenn Sie die Protokollierung auf Objektebene für Schreibdatenereignisse aktivieren, können Sie jeden einzelnen Objekt- (Datei-) Zugriff innerhalb eines S3-Buckets protokollieren. Durch die Aktivierung der Protokollierung auf Objektebene können Sie mithilfe von Amazon Events Datenkonformitätsanforderungen erfüllen, umfassende Sicherheitsanalysen durchführen AWS-Konto, bestimmte Muster des Benutzerverhaltens in Ihrem System überwachen und Maßnahmen gegen API-Aktivitäten auf Objektebene innerhalb Ihrer S3-Buckets ergreifen. CloudWatch Diese Steuerung führt `PASSED` zu einem Ergebnis, wenn Sie einen Trail mit mehreren Regionen konfigurieren, der nur Schreibvorgänge oder alle Arten von Datenereignissen für alle S3-Buckets protokolliert.

Abhilfe

Informationen zum Aktivieren der Protokollierung auf Objektebene für S3-Buckets finden Sie unter Aktivieren der CloudTrail Ereignisprotokollierung für S3-Buckets und Objekte im Amazon Simple Storage Service-Benutzerhandbuch.

[S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren

Verwandte Anforderungen: CIS Foundations Benchmark v3.0.0/3.9 AWS

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::::Account`

AWS Config Regel: **`cloudtrail-all-read-s3-data-event-check`**

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS-Konto über mindestens einen AWS CloudTrail Multiregions-Trail verfügt, der alle Lesedatenereignisse für Amazon S3 S3-Buckets protokolliert. Die Kontrolle schlägt fehl, wenn das Konto nicht über einen Multi-Regions-Trail verfügt, der Lesedatenereignisse für S3-Buckets protokolliert.

S3-Operationen auf Objektebene, wie, und `GetObject` `DeleteObject``PutObject`, werden als Datenereignisse bezeichnet. Standardmäßig protokolliert CloudTrail es keine Datenereignisse, aber Sie können Trails konfigurieren, um Datenereignisse für S3-Buckets zu protokollieren. Wenn Sie die Protokollierung auf Objektebene für Lesedatenereignisse aktivieren, können Sie jeden einzelnen Objekt- (Datei-) Zugriff innerhalb eines S3-Buckets protokollieren. Durch die Aktivierung der Protokollierung auf Objektebene können Sie mithilfe von Amazon Events Datenkonformitätsanforderungen erfüllen, umfassende Sicherheitsanalysen durchführen AWS-Konto, bestimmte Muster des Benutzerverhaltens in Ihrem System überwachen und Maßnahmen gegen API-Aktivitäten auf Objektebene innerhalb Ihrer S3-Buckets ergreifen. CloudWatch Diese Steuerung führt `PASSED` zu einem Ergebnis, wenn Sie einen Trail mit mehreren Regionen konfigurieren, der schreibgeschützte oder alle Arten von Datenereignissen für alle S3-Buckets protokolliert.

Abhilfe

Informationen zum Aktivieren der Protokollierung auf Objektebene für S3-Buckets finden Sie unter Aktivieren der CloudTrail Ereignisprotokollierung für S3-Buckets und Objekte im Amazon Simple Storage Service-Benutzerhandbuch.

SageMaker Amazon-Kontrollen

Diese Kontrollen beziehen sich auf SageMaker Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben

Verwandte Anforderungen: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.R5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.R5 AC-3. R5 AC-4, NIST.800-53.R5 AC-4 (21),

NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21)), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Hoch

Art der Ressource: `AWS::SageMaker::NotebookInstance`

AWS Config -Regel: `sagemaker-notebook-no-direct-internet-access`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob der direkte Internetzugang für eine SageMaker Notebook-Instanz deaktiviert ist. Die Steuerung schlägt fehl, wenn das `DirectInternetAccess` Feld für die Notebook-Instanz aktiviert ist.

Wenn Sie Ihre SageMaker Instance ohne VPC konfigurieren, ist der direkte Internetzugriff auf Ihrer Instance standardmäßig aktiviert. Sie sollten Ihre Instance mit einer VPC konfigurieren und die Standardeinstellung auf Deaktivieren — Zugriff auf das Internet über eine VPC ändern. Um Modelle von einem Notebook aus zu trainieren oder zu hosten, benötigen Sie Internetzugang. Um den Internetzugang zu aktivieren, muss Ihre VPC entweder über einen Schnittstellenendpunkt (AWS PrivateLink) oder ein NAT-Gateway und eine Sicherheitsgruppe verfügen, die ausgehende Verbindungen zulässt. Weitere Informationen zum Connect einer Notebook-Instance mit Ressourcen in einer VPC finden Sie unter Verbinden einer Notebook-Instance mit Ressourcen in einer VPC im Amazon SageMaker Developer Guide. Sie sollten auch sicherstellen, dass der Zugriff auf Ihre SageMaker Konfiguration nur auf autorisierte Benutzer beschränkt ist. Schränken Sie IAM-Berechtigungen ein, die es Benutzern ermöglichen, SageMaker Einstellungen und Ressourcen zu ändern.

Abhilfe

Sie können die Internetzugriffseinstellungen nicht ändern, nachdem Sie eine Notebook-Instanz erstellt haben. Stattdessen können Sie die Instanz mit blockiertem Internetzugang beenden, löschen und neu erstellen. Informationen zum Löschen einer Notebook-Instance, die direkten Internetzugang ermöglicht, finden Sie unter Verwenden von Notebook-Instances zum Erstellen von Modellen: Aufräumen im Amazon SageMaker Developer Guide. Informationen zum Neuerstellen einer

Notebook-Instance, die den Internetzugang verweigert, finden Sie unter Notebook-Instance erstellen. Wählen Sie für Netzwerk, Direkter Internetzugang die Option Deaktivieren — Zugriff auf das Internet über eine VPC.

[SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden

Verwandte Anforderungen: NIST.800-53.R5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 AC-6, NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9)

Kategorie: Schützen > Sichere Netzwerkkonfiguration > Ressourcen in VPC

Schweregrad: Hoch

Art der Ressource: `AWS::SageMaker::NotebookInstance`

AWS Config -Regel: `sagemaker-notebook-instance-inside-vpc`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Diese Steuerung prüft, ob eine SageMaker Amazon-Notebook-Instance in einer benutzerdefinierten Virtual Private Cloud (VPC) gestartet wird. Diese Steuerung schlägt fehl, wenn eine SageMaker Notebook-Instance nicht in einer benutzerdefinierten VPC oder in der SageMaker Service-VPC gestartet wird.

Subnetze sind ein Bereich von IP-Adressen innerhalb einer VPC. Wir empfehlen, Ihre Ressourcen wann immer möglich in einer benutzerdefinierten VPC aufzubewahren, um einen sicheren Netzwerkschutz Ihrer Infrastruktur zu gewährleisten. Eine Amazon VPC ist ein virtuelles Netzwerk, das Ihrem AWS-Konto gewidmet ist. Mit einer Amazon VPC können Sie den Netzwerkzugriff und die Internetverbindung Ihrer SageMaker Studio- und Notebook-Instances steuern.

Abhilfe

Sie können die VPC-Einstellung nicht ändern, nachdem Sie eine Notebook-Instanz erstellt haben. Stattdessen können Sie die Instanz beenden, löschen und neu erstellen. Anweisungen finden Sie

unter Verwenden von Notebook-Instances zum Erstellen von Modellen: Aufräumen im Amazon SageMaker Developer Guide.

[SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-6, NIST.800-53.R5 AC-6 (10), NIST.800-53.R5 AC-6 (2)

Kategorie: Schützen > Sichere Zugriffsverwaltung > Zugriffsbeschränkungen für Root-Benutzer

Schweregrad: Hoch

Art der Ressource: `AWS::SageMaker::NotebookInstance`

AWS Config -Regel: `sagemaker-notebook-instance-root-access-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob der Root-Zugriff für eine SageMaker Amazon-Notebook-Instance aktiviert ist. Die Steuerung schlägt fehl, wenn der Root-Zugriff für eine SageMaker Notebook-Instance aktiviert ist.

Unter Einhaltung des Prinzips der geringsten Rechte wird empfohlen, den Root-Zugriff auf Instanzressourcen zu beschränken, um eine unbeabsichtigte Überschreitung der Bereitstellungsberechtigungen zu vermeiden.

Abhilfe

Informationen zum Einschränken des Root-Zugriffs auf SageMaker Notebook-Instances finden Sie unter Steuern des Root-Zugriffs auf eine SageMaker Notebook-Instance im Amazon SageMaker Developer Guide.

[SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein

Verwandte Anforderungen: NIST.800-53.R5 CP-10, NIST.800-53.R5 SC-5, NIST.800-53.R5 SC-36, NIST.800-53.R5 SA-13

Kategorie: Wiederherstellung > Ausfallsicherheit > Hochverfügbarkeit

Schweregrad: Mittel

Art der Ressource: `AWS::SageMaker::EndpointConfig`

AWS Config -Regel: `sagemaker-endpoint-config-prod-instance-count`

Art des Zeitplans: Periodisch

Parameter: Keine

Diese Kontrolle prüft, ob Produktionsvarianten eines SageMaker Amazon-Endpunkts eine anfängliche Instanzzahl von mehr als 1 aufweisen. Die Kontrolle schlägt fehl, wenn die Produktionsvarianten des Endpunkts nur eine erste Instanz haben.

Produktionsvarianten, die mit einer Instance-Anzahl von mehr als 1 ausgeführt werden, ermöglichen eine Multi-AZ-Instance-Redundanz, die von verwaltet wird. SageMaker Die Bereitstellung von Ressourcen in mehreren Availability Zones ist eine AWS bewährte Methode, um eine hohe Verfügbarkeit innerhalb Ihrer Architektur zu gewährleisten. Hochverfügbarkeit hilft Ihnen, sich nach Sicherheitsvorfällen zu erholen.

> **Note**
>
> Diese Steuerung gilt nur für die instanzbasierte Endpunktkonfiguration.

Abhilfe

Weitere Informationen zu den Parametern der Endpunktkonfiguration finden Sie unter Erstellen einer Endpunktkonfiguration im Amazon SageMaker Developer Guide.

AWS Secrets Manager Steuerungen

Diese Steuerelemente beziehen sich auf Secrets Manager Manager-Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[SecretsManager.1] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3 (15)

Kategorie: Schutz > Sichere Entwicklung

Schweregrad: Mittel

Art der Ressource: `AWS::SecretsManager::Secret`

AWS Config -Regel: `secretsmanager-rotation-enabled-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`maximumAllowedRotationFrequency`	Höchstzulässige Anzahl von Tagen für die geheime Rotationsfrequenz	Ganzzahl	1 auf 365	Kein Standardwert

Dieses Steuerelement prüft, ob ein in gespeichertes Geheimnis mit automatischer Rotation konfiguriert AWS Secrets Manager ist. Die Steuerung schlägt fehl, wenn das Geheimnis nicht mit automatischer Rotation konfiguriert ist. Wenn Sie einen benutzerdefinierten Wert für den `maximumAllowedRotationFrequency` Parameter angeben, ist die Kontrolle nur erfolgreich, wenn das Geheimnis innerhalb des angegebenen Zeitfensters automatisch rotiert wird.

Secrets Manager hilft Ihnen, die Sicherheitslage Ihres Unternehmens zu verbessern. Zu den Geheimnissen gehören Datenbankanmeldedaten, Passwörter und API-Schlüssel von Drittanbietern. Sie können Secrets Manager verwenden, um Geheimnisse zentral zu speichern, Geheimnisse automatisch zu verschlüsseln, den Zugriff auf Geheimnisse zu kontrollieren und Geheimnisse sicher und automatisch zu rotieren.

Secrets Manager kann Secrets rotieren. Sie können die Rotation verwenden, um langfristige Geheimnisse durch kurzfristige zu ersetzen. Durch die Rotation Ihrer Geheimnisse wird begrenzt, wie lange ein nicht autorisierter Benutzer ein kompromittiertes Geheimnis verwenden kann. Aus diesem Grund sollten Sie Ihre Geheimnisse häufig wechseln. Weitere Informationen zur Rotation

findest du unter Rotation deiner AWS Secrets Manager Geheimnisse im AWS Secrets Manager Benutzerhandbuch.

Abhilfe

Informationen zum Aktivieren der automatischen Rotation für Secrets Manager-Secrets finden Sie unter Automatische Rotation für AWS Secrets Manager Secrets mithilfe der Konsole einrichten im AWS Secrets Manager Benutzerhandbuch. Sie müssen eine AWS Lambda Funktion für die Rotation auswählen und konfigurieren.

[SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3 (15)

Kategorie: Schutz > Sichere Entwicklung

Schweregrad: Mittel

Art der Ressource: `AWS::SecretsManager::Secret`

AWS Config -Regel: `secretsmanager-scheduled-rotation-success-check`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft anhand des Rotationsplans, ob ein AWS Secrets Manager Secret erfolgreich rotiert wurde. Wenn `RotationOccurringAsScheduled` ja, schlägt die Steuerung fehl`false`. Das Steuerelement wertet nur Geheimnisse aus, bei denen die Rotation aktiviert ist.

Secrets Manager hilft Ihnen, die Sicherheitslage Ihres Unternehmens zu verbessern. Zu den Geheimnissen gehören Datenbankanmeldedaten, Passwörter und API-Schlüssel von Drittanbietern. Sie können Secrets Manager verwenden, um Geheimnisse zentral zu speichern, Geheimnisse automatisch zu verschlüsseln, den Zugriff auf Geheimnisse zu kontrollieren und Geheimnisse sicher und automatisch zu rotieren.

Secrets Manager kann Secrets rotieren. Sie können die Rotation verwenden, um langfristige Geheimnisse durch kurzfristige zu ersetzen. Durch die Rotation Ihrer Geheimnisse wird begrenzt, wie lange ein nicht autorisierter Benutzer ein kompromittiertes Geheimnis verwenden kann. Aus diesem Grund sollten Sie Ihre Geheimnisse häufig wechseln.

Zusätzlich zur Konfiguration der automatischen Rotation sollten Sie sicherstellen, dass diese Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert werden.

Weitere Informationen zur Rotation finden Sie unter Rotation Ihrer AWS Secrets Manager Geheimnisse im AWS Secrets Manager Benutzerhandbuch.

Abhilfe

Wenn die automatische Rotation fehlschlägt, sind bei Secrets Manager möglicherweise Fehler bei der Konfiguration aufgetreten. Um Secrets in Secrets Manager zu rotieren, verwenden Sie eine Lambda-Funktion, die definiert, wie mit der Datenbank oder dem Dienst, dem das Geheimnis gehört, interagiert werden soll.

Hilfe zur Diagnose und Behebung häufiger Fehler im Zusammenhang mit der Rotation von Geheimnissen finden Sie unter Fehlerbehebung bei der AWS Secrets Manager Rotation von Geheimnissen im AWS Secrets Manager Benutzerhandbuch.

[SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3 (15)

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::SecretsManager::Secret`

AWS Config -Regel: `secretsmanager-secret-unused`

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`unusedForDays`	Maximale Anzahl von Tagen, an denen ein Geheimnis ungenutzt bleiben kann	Ganzzahl	1 auf 365	90

Dieses Steuerelement prüft, ob innerhalb des angegebenen Zeitraums auf ein AWS Secrets Manager Geheimnis zugegriffen wurde. Die Kontrolle schlägt fehl, wenn ein Geheimnis über den angegebenen Zeitraum hinaus nicht verwendet wird. Sofern Sie keinen benutzerdefinierten Parameterwert für den Zugriffszeitraum angeben, verwendet Security Hub einen Standardwert von 90 Tagen.

Das Löschen ungenutzter Geheimnisse ist genauso wichtig wie das Rotieren von Geheimnissen. Ungenutzte Geheimnisse können von ihren früheren Benutzern missbraucht werden, die keinen Zugriff mehr auf diese Geheimnisse benötigen. Wenn immer mehr Benutzer Zugriff auf ein Geheimnis erhalten, könnte es außerdem sein, dass jemand es falsch behandelt und an eine nicht autorisierte Stelle weitergegeben hat, was das Missbrauchsrisiko erhöht. Das Löschen ungenutzter Geheimnisse hilft dabei, Benutzern, die ihn nicht mehr benötigen, den geheimen Zugriff zu entziehen. Es hilft auch, die Kosten für die Verwendung von Secrets Manager zu senken. Daher ist es wichtig, ungenutzte Geheimnisse routinemäßig zu löschen.

Abhilfe

Informationen zum Löschen inaktiver Secrets Manager-Geheimnisse finden Sie unter Löschen eines AWS Secrets Manager Geheimnisses im AWS Secrets Manager Benutzerhandbuch.

[SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden

Verwandte Anforderungen: NIST.800-53.R5 AC-2 (1), NIST.800-53.R5 AC-3 (15)

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Mittel

Art der Ressource: `AWS::SecretsManager::Secret`

AWS Config -Regel: `secretsmanager-secret-periodic-rotation`

Art des Zeitplans: Periodisch

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`maxDaysSinceRotation`	Maximale Anzahl von Tagen, an denen ein Geheimnis unverändert bleiben kann	Ganzzahl	1 auf `180`	`90`

Dieses Steuerelement prüft, ob ein AWS Secrets Manager Geheimnis innerhalb des angegebenen Zeitrahmens mindestens einmal rotiert wurde. Die Kontrolle schlägt fehl, wenn ein Geheimnis nicht mindestens so häufig gewechselt wird. Sofern Sie keinen benutzerdefinierten Parameterwert für den Rotationszeitraum angeben, verwendet Security Hub einen Standardwert von 90 Tagen.

Rotierende Geheimnisse können Ihnen helfen, das Risiko einer unbefugten Verwendung Ihrer Geheimnisse in Ihrem zu verringern AWS-Konto. Beispiele hierfür sind Datenbankanmeldedaten, Passwörter, API-Schlüssel von Drittanbietern und sogar beliebiger Text. Wenn Sie Ihre Geheimnisse über einen längeren Zeitraum nicht ändern, ist es wahrscheinlicher, dass die Geheimnisse kompromittiert werden.

Je mehr Benutzer Zugriff auf ein Geheimnis erhalten, desto wahrscheinlicher kann es sein, dass jemand falsch damit umgegangen ist und es an eine nicht autorisierte Person weitergegeben hat. Secrets können über Protokolle und Cache-Daten durchsickern. Sie werden ggf. für Debug-Zwecke freigegeben und nicht geändert oder widerrufen, wenn das Debugging abgeschlossen ist. Aus all diesen Gründen sollten Secrets regelmäßig rotiert werden.

Sie können die automatische Rotation von Geheimnissen in konfigurieren. AWS Secrets Manager Mit der automatischen Rotation können Sie langfristige Geheimnisse durch kurzfristige ersetzen, wodurch das Risiko von Kompromissen erheblich reduziert wird. Wir empfehlen Ihnen, die automatische Rotation für Ihre Secrets Manager zu konfigurieren. Weitere Informationen finden Sie unter Rotieren von AWS Secrets Manager -Secrets im AWS Secrets Manager -Benutzerhandbuch.

Abhilfe

Informationen zum Aktivieren der automatischen Rotation für Secrets Manager-Secrets finden Sie unter Automatische Rotation für AWS Secrets Manager Secrets mithilfe der Konsole einrichten im AWS Secrets Manager Benutzerhandbuch. Sie müssen eine AWS Lambda Funktion für die Rotation auswählen und konfigurieren.

[SecretsManager.5] Secrets Manager Manager-Geheimnisse sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::SecretsManager::Secret`

AWS Config Regel: `tagged-secretsmanager-secret` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein AWS Secrets Manager Secret Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn das Geheimnis keine Tagschlüssel hat oder wenn es nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Geheimnis mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie

Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Secrets Manager Manager-Geheimnis finden Sie unter AWS Secrets Manager Taggeheimnisse im AWS Secrets Manager Benutzerhandbuch.

AWS Service Catalog Steuerungen

Diese Steuerelemente beziehen sich auf Service Catalog-Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden

Verwandte Anforderungen: NIst.800-53.R5 AC-3, NIST.800-53.R5 AC-4, NIST.800-53.R5 AC-6, NIst.800-53.R5 CM-8, NIst.800-53.R5 SC-7

Kategorie: Schutz > Sichere Zugriffsverwaltung

Schweregrad: Hoch

Art der Ressource: `AWS::ServiceCatalog::Portfolio`

AWS Config -Regel: `servicecatalog-shared-within-organization`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob AWS Service Catalog Portfolios innerhalb einer Organisation gemeinsam genutzt werden, wenn die Integration mit aktiviert AWS Organizations ist. Die Kontrolle schlägt fehl, wenn Portfolios nicht innerhalb einer Organisation gemeinsam genutzt werden.

Die Portfoliofreigabe nur innerhalb von Organizations trägt dazu bei, dass ein Portfolio nicht mit falschen Personen geteilt wird AWS-Konten. Um ein Servicekatalog-Portfolio mit einem Konto in einer Organisation zu teilen, empfiehlt Security Hub die Verwendung von `ORGANIZATION_MEMBER_ACCOUNT` anstelle von`ACCOUNT`. Dies vereinfacht die Verwaltung, da der Zugriff, der dem Konto gewährt wird, unternehmensweit geregelt wird. Wenn Sie aus geschäftlichen Gründen Service Catalog-Portfolios mit einem externen Konto teilen müssen, können Sie die Ergebnisse dieser Steuerung automatisch unterdrücken oder deaktivieren.

Abhilfe

Informationen zum Aktivieren der Portfoliofreigabe mit Organizations finden Sie unter Teilen mit AWS Organizations im Service Catalog-Administratorhandbuch

Steuerelemente von Amazon Simple Email Service

Diese Kontrollen beziehen sich auf Amazon SES SES-Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[SES.1] SES-Kontaktlisten sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::SES::ContactList`

AWS Config Regel: `tagged-ses-contactlist` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine Amazon SES SES-Kontaktliste Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Kontrolle schlägt fehl, wenn die Kontaktliste keine Tag-Schlüssel enthält oder wenn sie nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Kontaktliste mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Amazon SES-Kontaktliste finden Sie TagResourcein der Amazon SES API v2-Referenz.

[SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Kennzeichnung

Schweregrad: Niedrig

Art der Ressource: `AWS::SES::ConfigurationSet`

AWS Config Regel: `tagged-ses-configurationset` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob ein Amazon SES SES-Konfigurationssatz Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Die Steuerung schlägt fehl, wenn der Konfigurationssatz keine Tag-Schlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn der Konfigurationssatz mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem Amazon SES-Konfigurationssatz finden Sie TagResourcein der Amazon SES API v2-Referenz.

Steuerelemente von Amazon Simple Notification Service

Diese Kontrollen beziehen sich auf Amazon SNS SNS-Ressourcen.

Diese Kontrollen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[SNS.1] SNS-Themen sollten im Ruhezustand wie folgt verschlüsselt werden AWS KMS

> **Important**
>
> Security Hub hat diese Kontrolle im April 2024 aus dem Standard AWS Foundational Security Best Practices entfernt, sie ist jedoch weiterhin im Standard NIST SP 800-53 Rev. 5 enthalten. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::SNS::Topic`

AWS Config -Regel: `sns-encrypted-kms`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob ein Amazon SNS SNS-Thema im Ruhezustand mithilfe von Schlüsseln verschlüsselt ist, die in AWS Key Management Service (AWS KMS) verwaltet werden. Die Steuerung schlägt fehl, wenn das SNS-Thema keinen KMS-Schlüssel für die serverseitige Verschlüsselung (SSE) verwendet. Standardmäßig speichert SNS Nachrichten und Dateien mithilfe der Festplattenverschlüsselung. Um diese Kontrolle zu bestehen, müssen Sie stattdessen einen KMS-Schlüssel für die Verschlüsselung verwenden. Dies fügt eine zusätzliche Sicherheitsebene hinzu und bietet mehr Flexibilität bei der Zugriffskontrolle.

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass auf Daten, die auf der Festplatte gespeichert sind, von einem Benutzer zugegriffen wird, für den kein Benutzer authentifiziert ist. AWS API-Berechtigungen sind erforderlich, um die Daten zu entschlüsseln, bevor

sie gelesen werden können. Wir empfehlen, SNS-Themen mit KMS-Schlüsseln zu verschlüsseln, um eine zusätzliche Sicherheitsebene zu gewährleisten.

Abhilfe

Informationen zur Aktivierung von SSE für ein SNS-Thema finden Sie unter Serverseitige Verschlüsselung (SSE) für ein Amazon SNS SNS-Thema aktivieren im Amazon Simple Notification Service Developer Guide. Bevor Sie SSE verwenden können, müssen Sie außerdem AWS KMS key Richtlinien konfigurieren, die die Verschlüsselung von Themen sowie die Verschlüsselung und Entschlüsselung von Nachrichten ermöglichen. Weitere Informationen finden Sie unter Konfiguration von AWS KMS Berechtigungen im Amazon Simple Notification Service Developer Guide.

[SNS.2] Die Protokollierung des Lieferstatus sollte für Benachrichtigungen aktiviert sein, die an ein Thema gesendet werden

> **Important**
>
> Security Hub hat diese Kontrolle im April 2024 eingestellt. Weitere Informationen finden Sie unter Änderungsprotokoll für Security Hub-Steuerelemente.

Verwandte Anforderungen: NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::SNS::Topic`

AWS Config -Regel: `sns-topic-message-delivery-notification-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung für den Lieferstatus von Benachrichtigungen aktiviert ist, die an ein Amazon SNS SNS-Thema für die Endgeräte gesendet werden. Diese Kontrolle schlägt fehl, wenn die Benachrichtigung über den Lieferstatus von Nachrichten nicht aktiviert ist.

Die Protokollierung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Diensten. Die Protokollierung des Nachrichtenzustellungsstatus hilft dabei, betriebliche Erkenntnisse wie die folgenden zu gewinnen:

- Kenntnis, ob eine Mitteilung an den Amazon SNS-Endpunkt gesendet wurde.
- Ermittlung der Antwort, die vom Amazon SNS-Endpunkt an Amazon SNS gesendet wurde.
- Bestimmung der Verweildauer der Nachricht (die Zeit zwischen dem Veröffentlichungszeitstempel und der Übergabe an einen Amazon SNS SNS-Endpunkt).

Abhilfe

Informationen zur Konfiguration der Versandstatusprotokollierung für ein Thema finden Sie unter Amazon SNS SNS-Nachrichtenzustellungsstatus im Amazon Simple Notification Service Developer Guide.

[SNS.3] SNS-Themen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::SNS::Topic`

AWS Config Regel: `tagged-sns-topic` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob ein Amazon SNS SNS-Thema Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Das Steuerelement schlägt fehl, wenn das Thema keine Tag-Schlüssel hat oder wenn es nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn das Thema mit keinem Schlüssel markiert ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einem SNS-Thema finden Sie unter Konfiguration von Amazon SNS SNS-Themen-Tags im Amazon Simple Notification Service Developer Guide.

Steuerelemente von Amazon Simple Queue Service

Diese Kontrollen beziehen sich auf Amazon SQS SQS-Ressourcen.

Diese Steuerungen sind möglicherweise nicht in allen AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten im Ruhezustand

Schweregrad: Mittel

Art der Ressource: `AWS::SQS::Queue`

AWS Config Regel: `sqs-queue-encrypted` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine Amazon SQS SQS-Warteschlange im Ruhezustand verschlüsselt ist. Die Steuerung schlägt fehl, wenn die Warteschlange nicht mit einem von SQL verwalteten Schlüssel (SSE-SQS) oder einem AWS Key Management Service () Schlüssel (SSE-KMS) verschlüsselt ist.AWS KMS

Durch die Verschlüsselung von Daten im Ruhezustand wird das Risiko verringert, dass ein nicht autorisierter Benutzer auf Daten zugreift, die auf der Festplatte gespeichert sind. Die serverseitige Verschlüsselung (SSE) schützt den Inhalt von Nachrichten in SQS-Warteschlangen mithilfe von SQS-verwalteten Verschlüsselungsschlüsseln (SSE-SQS) oder Schlüsseln (SSE-KMS). AWS KMS

Abhilfe

Informationen zur Konfiguration von SSE für eine SQS-Warteschlange finden Sie unter Konfiguration der serverseitigen Verschlüsselung (SSE) für eine Warteschlange (Konsole) im Amazon Simple Queue Service Developer Guide.

[SQS.2] SQS-Warteschlangen sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::SQS::Queue`

AWS Config Regel: `tagged-sqs-queue` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	`No default value`

Dieses Steuerelement prüft, ob eine Amazon SQS SQS-Warteschlange Tags mit den spezifischen Schlüsseln enthält, die im Parameter `requiredTagKeys` definiert sind. Die Steuerung schlägt fehl, wenn die Warteschlange keine Tag-Schlüssel hat oder wenn sie nicht alle im Parameter `requiredTagKeys` angegebenen Schlüssel enthält. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn die Warteschlange mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen

anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer vorhandenen Warteschlange mithilfe der Amazon SQS SQS-Konsole finden Sie unter Konfiguration von Kostenzuweisungs-Tags für eine Amazon SQS SQS-Warteschlange (Konsole) im Amazon Simple Queue Service Developer Guide.

AWS Step Functions Kontrollen

Diese Steuerelemente beziehen sich auf die Ressourcen von Step Functions.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::StepFunctions::StateMachine`

AWS Config -Regel: `step-functions-state-machine-logging-enabled`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`logLevel`	Minimale Protokollierungsebene	Enum	`ALL`, `ERROR`, `FATAL`	Kein Standardwert

Mit dieser Steuerung wird geprüft, ob bei einer AWS Step Functions Zustandsmaschine die Protokollierung aktiviert ist. Die Steuerung schlägt fehl, wenn auf einer Zustandsmaschine die Protokollierung nicht aktiviert ist. Wenn Sie einen benutzerdefinierten Wert für den `logLevel` Parameter angeben, wird die Steuerung nur erfolgreich ausgeführt, wenn für die Zustandsmaschine die angegebene Protokollierungsebene aktiviert ist.

Die Überwachung hilft Ihnen dabei, die Zuverlässigkeit, Verfügbarkeit und Leistung von Step Functions aufrechtzuerhalten. Sie sollten so viele Überwachungsdaten sammeln AWS-Services , wie Sie verwenden, damit Sie Fehler an mehreren Punkten leichter debuggen können. Wenn Sie eine Protokollierungskonfiguration für Ihre Step Functions Functions-Zustandsmaschinen definiert haben, können Sie den Ausführungsverlauf und die Ergebnisse in Amazon CloudWatch Logs verfolgen. Optional können Sie nur Fehler oder schwerwiegende Ereignisse verfolgen.

Abhilfe

Informationen zum Aktivieren der Protokollierung für eine Step Functions Functions-Zustandsmaschine finden Sie unter Protokollierung konfigurieren im AWS Step Functions Entwicklerhandbuch.

[StepFunctions.2] Die Aktivitäten von Step Functions sollten markiert werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::StepFunctions::Activity`

AWS Config Regel: `tagged-stepfunctions-activity` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.	StringList	Liste der Tags, die die AWS Anforderungen erfüllen	Kein Standardwert

Dieses Steuerelement prüft, ob eine AWS Step Functions Aktivität Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn die Aktivität keine Tag-Schlüssel hat oder wenn nicht alle im Parameter angegebenen Schlüssel vorhanden sind`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tag-Schlüssel vorhanden ist, und schlägt fehl, wenn die Aktivität mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

Informationen zum Hinzufügen von Tags zu einer Step Functions-Aktivität finden Sie unter Tagging in Step Functions im AWS Step Functions Entwicklerhandbuch.

AWS Transfer Family Steuerungen

Diese Steuerelemente beziehen sich auf die Ressourcen von Transfer Family.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[Transfer.1] AWS Transfer Family -Workflows sollten mit Tags versehen werden

Kategorie: Identifizieren > Inventar > Tagging

Schweregrad: Niedrig

Art der Ressource: `AWS::Transfer::Workflow`

AWS Config Regel: `tagged-transfer-workflow` (benutzerdefinierte Security Hub Hub-Regel)

Zeitplantyp: Änderung wurde ausgelöst

Parameter:

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
`requiredTagKeys`	Liste der -Tag-Schlüssel, die die evaluierte Ressource	StringList	Liste der Tags, die	`No default value`

Parameter	Beschreibung	Typ	Zulässige benutzerdefinierte Werte	Security Hub Hub-Standardwert
	enthalten muss. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.		die AWS Anforderungen erfüllen	

Dieses Steuerelement prüft, ob ein AWS Transfer Family Workflow Tags mit den spezifischen Schlüsseln enthält, die im Parameter definiert sind`requiredTagKeys`. Das Steuerelement schlägt fehl, wenn der Workflow keine Tagschlüssel hat oder wenn er nicht alle im Parameter angegebenen Schlüssel enthält`requiredTagKeys`. Wenn der Parameter `requiredTagKeys` nicht angegeben wird, prüft das Steuerelement nur, ob ein Tagschlüssel vorhanden ist, und schlägt fehl, wenn der Workflow mit keinem Schlüssel gekennzeichnet ist. Systemtags, die automatisch angewendet werden und mit beginnen`aws:`, werden ignoriert.

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Sie besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Mithilfe von Tags können Sie Ressourcen identifizieren, organisieren, suchen und filtern. Mithilfe von Stichwörtern können Sie außerdem nachvollziehen, welche Aktionen und Benachrichtigungen von Ressourcenbesitzern verantwortlich sind. Wenn Sie Tagging verwenden, können Sie die attributebasierte Zugriffskontrolle (ABAC) als Autorisierungsstrategie implementieren, bei der Berechtigungen auf der Grundlage von Tags definiert werden. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und Ressourcen anhängen. AWS Sie können eine einzelne ABAC-Richtlinie oder einen separaten Satz von Richtlinien für Ihre IAM-Prinzipale erstellen. Sie können diese ABAC-Richtlinien so entwerfen, dass Operationen möglich sind, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

> **Note**
>
> Fügen Sie keine persönlich identifizierbaren Informationen (PII) oder andere vertrauliche oder sensible Informationen zu Tags hinzu. Tags sind für viele zugänglich AWS-Services, darunter

AWS Billing. Weitere bewährte Methoden zum Taggen finden Sie unter Taggen Ihrer AWS Ressourcen in der. Allgemeine AWS-Referenz

Abhilfe

So fügen Sie Stichwörter zu einem Transfer Family Family-Workflow hinzu (Konsole)

1. Öffnen Sie die AWS Transfer Family Konsole.
2. Wählen Sie im Navigationsbereich Workflows aus. Wählen Sie dann den Workflow aus, den Sie taggen möchten.
3. Wählen Sie Tags verwalten und fügen Sie die Tags hinzu.

[Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden

Verwandte Anforderungen: NIST.800-53.R5 CM-7, NIST.800-53.R5 IA-5, NIST.800-53.R5 SC-8

Kategorie: Schutz > Datenschutz > Verschlüsselung von Daten währen der Übertragung

Schweregrad: Mittel

Art der Ressource: `AWS::Transfer::Server`

AWS Config -Regel: `transfer-family-server-no-ftp`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob ein AWS Transfer Family Server ein anderes Protokoll als FTP für die Endpunktverbindung verwendet. Die Steuerung schlägt fehl, wenn der Server das FTP-Protokoll verwendet, damit ein Client eine Verbindung zum Serverendpunkt herstellt.

FTP (File Transfer Protocol) stellt die Endpunktverbindung über unverschlüsselte Kanäle her, sodass Daten, die über diese Kanäle gesendet werden, abgefangen werden können. Die Verwendung von SFTP (SSH File Transfer Protocol), FTPS (File Transfer Protocol Secure) oder AS2 (Applicability Statement 2) bietet eine zusätzliche Sicherheitsebene, indem Ihre Daten während der Übertragung verschlüsselt werden, und kann dazu beitragen, potenzielle Angreifer daran zu

hindern, Netzwerkverkehr mit person-in-the-middle oder ähnlichen Angriffen zu belauschen oder zu manipulieren.

Abhilfe

Informationen zum Ändern des Protokolls für einen Transfer Family Family-Server finden Sie unter Bearbeiten der Dateiübertragungsprotokolle im AWS Transfer Family Benutzerhandbuch.

AWS WAF steuert

Diese Kontrollen beziehen sich auf AWS WAF Ressourcen.

Diese Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.

[WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-3. R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::WAF::WebACL`

AWS Config -Regel: `waf-classic-logging-enabled`

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung für eine AWS WAF globale Web-ACL aktiviert ist. Dieses Steuerelement schlägt fehl, wenn die Protokollierung für die Web-ACL nicht aktiviert ist.

Die Protokollierung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von AWS WAF Global. Sie ist in vielen Unternehmen eine Geschäfts- und Compliance-Anforderung und ermöglicht es Ihnen, Fehler beim Verhalten von Anwendungen zu beheben. Es enthält auch detaillierte Informationen über den Datenverkehr, der von der angehängten Web-ACL analysiert wird AWS WAF.

Abhilfe

Informationen zum Aktivieren der Protokollierung für eine AWS WAF Web-ACL finden Sie unter Logging Web-ACL-Verkehrsinformationen im AWS WAF Developer Guide.

[WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben

Verwandte Anforderungen: NIst.800-53.R5 AC-4 (21), NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIst.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (21)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::WAFRegional::Rule`

AWS Config -Regel: `waf-regional-rule-not-empty`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF Regionalregel mindestens eine Bedingung hat. Die Steuerung schlägt fehl, wenn in einer Regel keine Bedingungen erfüllt sind.

Eine regionale WAF-Regel kann mehrere Bedingungen enthalten. Die Bedingungen der Regel ermöglichen die Überprüfung des Verkehrs und das Ergreifen einer definierten Aktion (Zulassen, Blockieren oder Zählen). Ohne jegliche Bedingungen wird der Verkehr ohne Inspektion weitergeleitet. Eine WAF-Regionalregel ohne Bedingungen, aber mit einem Namen oder Tag, der auf Zulassen, Blockieren oder Zählen hindeutet, könnte zu der falschen Annahme führen, dass eine dieser Aktionen stattfindet.

Abhilfe

Informationen zum Hinzufügen einer Bedingung zu einer leeren Regel finden Sie unter Hinzufügen und Entfernen von Bedingungen in einer Regel im AWS WAF Entwicklerhandbuch.

[WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben

Verwandte Anforderungen: NIST.800-53.R5 AC-4 (21), NIST.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (21)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::WAFRegional::RuleGroup`

AWS Config -Regel: `waf-regional-rulegroup-not-empty`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF regionale Regelgruppe mindestens eine Regel hat. Die Steuerung schlägt fehl, wenn in einer Regelgruppe keine Regeln vorhanden sind.

Eine regionale WAF-Regelgruppe kann mehrere Regeln enthalten. Die Bedingungen der Regel ermöglichen die Überprüfung des Datenverkehrs und das Ergreifen einer definierten Aktion (Zulassen, Blockieren oder Zählen). Ohne Regeln passiert der Verkehr ohne Inspektion. Eine regionale WAF-Regelgruppe ohne Regeln, aber mit einem Namen oder Tag, der auf Zulassen, Blockieren oder Zählen hindeutet, könnte zu der falschen Annahme führen, dass eine dieser Aktionen stattfindet.

Abhilfe

Informationen zum Hinzufügen von Regeln und Regelbedingungen zu einer leeren Regelgruppe finden Sie unter Hinzufügen und Löschen von Regeln aus einer AWS WAF klassischen Regelgruppe und Hinzufügen und Entfernen von Bedingungen in einer Regel im AWS WAF Entwicklerhandbuch.

[WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::WAFRegional::WebACL`

AWS Config -Regel: `waf-regional-webacl-not-empty`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF Classic Regional Web-ACL WAF-Regeln oder WAF-Regelgruppen enthält. Dieses Steuerelement schlägt fehl, wenn eine Web-ACL keine WAF-Regeln oder Regelgruppen enthält.

Eine regionale WAF-Web-ACL kann eine Sammlung von Regeln und Regelgruppen enthalten, die Webanfragen prüfen und kontrollieren. Wenn eine Web-ACL leer ist, kann der Web-Traffic je nach Standardaktion weitergeleitet werden, ohne von der WAF erkannt oder bearbeitet zu werden.

Abhilfe

Informationen zum Hinzufügen von Regeln oder Regelgruppen zu einer leeren AWS WAF Classic Regional Web-ACL finden Sie unter Bearbeiten einer Web-ACL im AWS WAF Entwicklerhandbuch.

[WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::WAF::Rule`

AWS Config -Regel: `waf-global-rule-not-empty`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF globale Regel Bedingungen enthält. Das Steuerelement schlägt fehl, wenn in einer Regel keine Bedingungen erfüllt sind.

Eine globale WAF-Regel kann mehrere Bedingungen enthalten. Die Bedingungen einer Regel ermöglichen die Überprüfung des Datenverkehrs und die Durchführung einer definierten Aktion (Zulassen, Blockieren oder Zählen). Ohne jegliche Bedingungen wird der Verkehr ohne Inspektion weitergeleitet. Eine globale WAF-Regel ohne Bedingungen, aber mit einem Namen oder Tag, der auf Zulassen, Blockieren oder Zählen hindeutet, könnte zu der falschen Annahme führen, dass eine dieser Aktionen stattfindet.

Abhilfe

Anweisungen zum Erstellen einer Regel und zum Hinzufügen von Bedingungen finden Sie unter Regel erstellen und Bedingungen hinzufügen im AWS WAF Entwicklerhandbuch.

[WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben

Verwandte Anforderungen: NIST.800-53.R5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::WAF::RuleGroup`

AWS Config -Regel: `waf-global-rulegroup-not-empty`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF globale Regelgruppe mindestens eine Regel hat. Das Steuerelement schlägt fehl, wenn innerhalb einer Regelgruppe keine Regeln vorhanden sind.

Eine globale WAF-Regelgruppe kann mehrere Regeln enthalten. Die Bedingungen der Regel ermöglichen die Überprüfung des Datenverkehrs und das Ergreifen einer definierten Aktion (Zulassen, Blockieren oder Zählen). Ohne Regeln passiert der Verkehr ohne Inspektion. Eine globale WAF-Regelgruppe ohne Regeln, aber mit einem Namen oder Tag, der auf Zulassen, Blockieren oder Zählen hindeutet, könnte zu der falschen Annahme führen, dass eine dieser Aktionen stattfindet.

Abhilfe

Anweisungen zum Hinzufügen einer Regel zu einer Regelgruppe finden Sie unter Creating an AWS WAF Classic Rule Group im AWS WAF Developer Guide.

[WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Verwandte Anforderungen: NIst.800-53.R5 AC-4 (21), NIST.800-53.R5 SC-7, NIst.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (21)

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::WAF::WebACL`

AWS Config -Regel: `waf-global-webacl-not-empty`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF globale Web-ACL mindestens eine WAF-Regel oder WAF-Regelgruppe enthält. Die Steuerung schlägt fehl, wenn eine Web-ACL keine WAF-Regeln oder Regelgruppen enthält.

Eine globale WAF-Web-ACL kann eine Sammlung von Regeln und Regelgruppen enthalten, die Webanfragen prüfen und kontrollieren. Wenn eine Web-ACL leer ist, kann der Web-Traffic je nach Standardaktion weitergeleitet werden, ohne von der WAF erkannt oder bearbeitet zu werden.

Abhilfe

Informationen zum Hinzufügen von Regeln oder Regelgruppen zu einer leeren AWS WAF globalen Web-ACL finden Sie unter Bearbeiten einer Web-ACL im AWS WAF Entwicklerhandbuch. Wählen Sie für Filter die Option Global (CloudFront).

[WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Verwandte Anforderungen: NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2

Kategorie: Schutz > Sichere Netzwerkkonfiguration

Schweregrad: Mittel

Art der Ressource: `AWS::WAFv2::WebACL`

AWS Config -Regel: `wafv2-webacl-not-empty`

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob eine AWS WAF V2-Web-Zugriffskontrollliste (Web-ACL) mindestens eine Regel oder Regelgruppe enthält. Die Steuerung schlägt fehl, wenn eine Web-ACL keine Regeln oder Regelgruppen enthält.

Eine Web-ACL gibt Ihnen eine detaillierte Kontrolle über alle HTTP (S) -Webanfragen, auf die Ihre geschützte Ressource reagiert. Eine Web-ACL sollte eine Sammlung von Regeln und Regelgruppen enthalten, die Webanfragen prüfen und kontrollieren. Wenn eine Web-ACL leer ist, kann der Web-Traffic AWS WAF je nach Standardaktion weitergeleitet werden, ohne dass er erkannt oder bearbeitet wird.

Abhilfe

Informationen zum Hinzufügen von Regeln oder Regelgruppen zu einer leeren WAF2-Web-ACL finden Sie unter Bearbeiten einer Web-ACL im AWS WAF Entwicklerhandbuch.

[WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein

Verwandte Anforderungen: NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-3. R5 CA-7, NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Niedrig

Art der Ressource: `AWS::WAFv2::WebACL`

AWS Config Regel: **`wafv2-logging-enabled`**

Art des Zeitplans: Periodisch

Parameter: Keine

Dieses Steuerelement prüft, ob die Protokollierung für eine AWS WAF V2-Webzugriffskontrollliste (Web-ACL) aktiviert ist. Diese Kontrolle schlägt fehl, wenn die Protokollierung für die Web-ACL deaktiviert ist.

Die Protokollierung gewährleistet die Zuverlässigkeit, Verfügbarkeit und Leistung von AWS WAF. Darüber hinaus ist die Protokollierung in vielen Organisationen eine Geschäfts- und Compliance-Anforderung. Indem Sie den von Ihrer Web-ACL analysierten Datenverkehr protokollieren, können Sie Fehler beim Verhalten von Anwendungen beheben.

Abhilfe

Informationen zur Aktivierung der Protokollierung für eine AWS WAF Web-ACL finden Sie unter Verwaltung der Protokollierung für eine Web-ACL im AWS WAF Entwicklerhandbuch.

Für [WAF.12] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch

Verwandte Anforderungen: NIST.800-53.R5 AC-4 (26), NIST.800-53.R5 AU-10, NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-3. R5 CA-7, NIST.800-53.R5 SC-7 (10), NIST.800-53.R5 SC-7 (9), NIST.800-53.R5 SI-7 (8)

Kategorie: Identifizieren > Protokollierung

Schweregrad: Mittel

Art der Ressource: `AWS::WAFv2::RuleGroup`

AWS Config Regel: **`wafv2-rulegroup-logging-enabled`**

Art des Zeitplans: Änderung wurde ausgelöst

Parameter: Keine

Dieses Steuerelement prüft, ob für eine AWS WAF Regel oder Regelgruppe CloudWatch Amazon-Metriken aktiviert sind. Die Kontrolle schlägt fehl, wenn für die Regel oder Regelgruppe keine CloudWatch Metriken aktiviert sind.

Durch die Konfiguration von CloudWatch Metriken AWS WAF für Regeln und Regelgruppen erhalten Sie Einblick in den Verkehrsfluss. Sie können sehen, welche ACL-Regeln ausgelöst werden und welche Anfragen akzeptiert und blockiert werden. Diese Sichtbarkeit kann Ihnen helfen, böswillige Aktivitäten auf Ihren verknüpften Ressourcen zu erkennen.

Abhilfe

Rufen Sie die UpdateRuleGroupAPI auf, um CloudWatch Metriken für eine AWS WAF Regelgruppe zu aktivieren. Rufen Sie die UpdateWebACL-API auf, um CloudWatch Metriken für eine AWS WAF Regel zu aktivieren. Stellen Sie das `CloudWatchMetricsEnabled` Feld auf ein. `true` Wenn Sie die AWS WAF Konsole verwenden, um Regeln oder Regelgruppen zu erstellen, werden CloudWatch Metriken automatisch aktiviert.

Sicherheitskontrollen anzeigen und verwalten

Eine Kontrolle ist eine Schutzmaßnahme innerhalb eines Sicherheitsstandards, die einem Unternehmen hilft, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationen zu schützen. In Security Hub bezieht sich ein Steuerelement auf eine bestimmte AWS Ressource.

Ansicht „Konsolidierte Kontrollen“

Auf der Seite „Steuerungen“ der Security Hub Hub-Konsole werden alle derzeit verfügbaren Steuerelemente angezeigt AWS-Region (Sie können Kontrollen im Kontext eines Standards anzeigen, indem Sie die Seite Sicherheitsstandards aufrufen und einen aktivierten Standard auswählen). Security Hub weist Kontrollen standardübergreifend eine einheitliche Sicherheitssteuerungs-ID, einen Titel und eine Beschreibung zu. Die Kontroll-IDs enthalten die relevante AWS-Service und eine eindeutige Nummer (z. B. CodeBuild .3).

Die folgenden Informationen sind auf der Kontrollseite der Security Hub Hub-Konsole verfügbar:

- Eine allgemeine Sicherheitsbewertung, die auf dem Anteil der bestandenen Kontrollen im Vergleich zur Gesamtzahl der aktivierten Kontrollen mit Daten basiert
- Der Prozentsatz der fehlgeschlagenen Sicherheitsüberprüfungen an allen aktivierten Kontrollen
- Die Anzahl der bestandenen und fehlgeschlagenen Sicherheitsprüfungen für Kontrollen mit unterschiedlichem Schweregrad
- Eine Liste von Kontrollen, die je nach Aktivierungsstatus in verschiedene Registerkarten unterteilt sind. Verfügbare Steuerelemente, die für keinen Ihrer aktivierten Standards gelten, werden in der Spalte Deaktiviert angezeigt. Unverarbeitete Steuerelemente, z. B. solche, die in Ihrer aktuellen Region nicht verfügbar sind, werden in der Spalte Keine Daten angezeigt. Die Anzahl der Steuerelemente in der Spalte Alle entspricht der Summe der Steuerelemente in den Datenspalten Fehlgeschlagen, Unbekannt, Bestanden, Deaktiviert und Keine Daten.

Auf der Seite „Kontrollen“ können Sie ein Steuerelement auswählen, um dessen Details anzuzeigen und anhand der von dem Steuerelement generierten Ergebnisse Maßnahmen zu ergreifen. Auf dieser Seite können Sie auch eine Sicherheitskontrolle in Ihrem aktuellen AWS-Konto und aktivieren oder deaktivieren AWS-Region. Die Aktivierungs- und Deaktivierungsaktionen auf der Seite „Kontrollen“ gelten für alle Standards. Weitere Informationen finden Sie unter Aktivierung und Deaktivierung von Steuerungen in allen Standards.

Bei Administratorkonten gibt die Seite „Kontrollen“ den Status der Kontrollen für alle Mitgliedskonten wieder. Wenn eine Kontrollüberprüfung in mindestens einem Mitgliedskonto fehlschlägt, wird die Kontrolle auf der Seite „Kontrollen“ auf der Registerkarte Fehlgeschlagen angezeigt. Wenn Sie eine Aggregationsregion festgelegt haben, zeigt die Seite „Steuerelemente“ den Status der Kontrollen in allen verknüpften Regionen an. Wenn eine Kontrollüberprüfung in mindestens einer verknüpften Region fehlschlägt, wird das Steuerelement auf der Seite „Steuerelemente“ auf der Registerkarte Fehlgeschlagen angezeigt.

Die Ansicht konsolidierter Kontrollen führt zu Änderungen an den Kontrollsuchfeldern im AWS Security Finding Format (ASFF), die sich auf Workflows auswirken können. Weitere Informationen finden Sie unter Ansicht der konsolidierten Kontrollen — ASFF-Änderungen.

Allgemeine Sicherheitsbewertung für Kontrollen

Auf der Seite „Kontrollen“ wird eine Gesamtsicherheitsbewertung von 0 bis 100 Prozent angezeigt. Die Gesamtsicherheitsbewertung wird auf der Grundlage des Anteils der bestandenen Kontrollen im Vergleich zur Gesamtzahl der aktivierten Kontrollen mit Daten berechnet.

> **Note**
>
> Um die Gesamtsicherheitsbewertung für Kontrollen anzuzeigen, müssen Sie der IAM-Rolle, die Sie für den **`BatchGetControlEvaluations`**Zugriff auf Security Hub verwenden, die Berechtigung zum Aufrufen hinzufügen. Diese Berechtigung ist nicht erforderlich, um Sicherheitsbewertungen für bestimmte Standards einzusehen.

Wenn Sie Security Hub aktivieren, berechnet Security Hub die anfängliche Sicherheitsbewertung innerhalb von 30 Minuten nach Ihrem ersten Besuch der Übersichtsseite oder der Seite Sicherheitsstandards in der Security Hub Hub-Konsole. In den Regionen China und kann es bis zu 24 Stunden dauern, bis zum ersten Mal Sicherheitsbewertungen generiert werden. AWS GovCloud (US) Region Bewertungen werden nur für Standards generiert, die aktiviert sind, wenn Sie diese Seiten besuchen. Verwenden Sie den `GetEnabledStandards`API-Vorgang, um eine Liste der derzeit aktivierten Standards anzuzeigen. Darüber hinaus muss die AWS Config Ressourcenaufzeichnung konfiguriert werden, damit die Ergebnisse angezeigt werden. Die Gesamtsicherheitsbewertung ist der Durchschnitt der Standardsicherheitsbewertungen.

Nach der erstmaligen Generierung der Ergebnisse aktualisiert Security Hub die Sicherheitswerte alle 24 Stunden. Security Hub zeigt einen Zeitstempel an, der angibt, wann eine Sicherheitsbewertung zuletzt aktualisiert wurde.

Wenn Sie eine Aggregationsregion festgelegt haben, spiegelt die Gesamtsicherheitsbewertung die Kontrollergebnisse der verknüpften Regionen wider.

Themen

- Kontrollkategorien
- Aktivierung und Deaktivierung von Steuerungen in allen Standards

- Automatisches Aktivieren neuer Steuerelemente in aktivierten Standards
- Benutzerdefinierte Steuerungsparameter
- Security Hub-Steuerelemente, die Sie möglicherweise deaktivieren möchten
- Details für ein Steuerelement anzeigen
- Die Liste der Steuerelemente filtern und sortieren
- Kontrollergebnisse anzeigen und entsprechende Maßnahmen ergreifen

Kontrollkategorien

Jedem Steuerelement ist eine Kategorie zugewiesen. Die Kategorie einer Kontrolle spiegelt die Sicherheitsfunktion wider, auf die die Kontrolle angewendet wird.

Der Kategoriewert enthält die Kategorie, die Unterkategorie innerhalb der Kategorie und optional einen Klassifikator innerhalb der Unterkategorie. Beispielsweise:

- Identifizieren > Inventar
- Schützen > Datenschutz > Verschlüsselung von Daten bei der Übertragung

Hier finden Sie die Beschreibungen der verfügbaren Kategorien, Unterkategorien und Klassifikatoren.

Identifizieren

Entwickeln Sie die organisatorische Grundlagen für das Management von Cybersicherheitsrisiken für Systeme, Assets, Daten und Funktionen.

-Bestand

> Hat der Service die richtigen Ressourcen-Tagging-Strategien implementiert? Schließen die Tagging-Strategien den Ressourcenbesitzer ein?
>
> Welche Ressourcen werden vom Service genutzt? Sind sie für diesen Service genehmigte Ressourcen?
>
> Haben Sie Einblick in den genehmigten Bestand? Verwenden Sie beispielsweise Dienste wie Amazon EC2 Systems Manager und Service Catalog?

Protokollierung

Haben Sie die gesamte relevante Protokollierung für den Service sicher aktiviert? Beispiele für Protokolldateien sind die folgenden:

- Amazon VPC-Flussprotokolle
- Zugriffsprotokolle für Elastic Load Balancing
- CloudFront Amazon-Protokolle
- CloudWatch Amazon-Protokolle
- Protokollierung durch Amazon Relational Database Service
- Langsame Indexprotokolle von Amazon OpenSearch Service
- X-Ray-Nachverfolgung
- AWS Directory Service Protokolle
- AWS Config Artikel
- Snapshots

Schutz

Entwicklung und Implementierung geeigneter Sicherheitsvorkehrungen, um die Bereitstellung kritischer Infrastrukturservices und sicherer Codierungspraktiken zu gewährleisten.

Sichere Zugriffsverwaltung

Verwendet der Service in seinen IAM- oder Ressourcenrichtlinien Verfahren mit den geringsten Rechten?

Sind Passwörter und Secrets ausreichend komplex? Werden sie angemessen rotiert?

Verwendet der Service Multi-Factor Authentication (MFA)?

Vermeidet der Dienst den Root-Benutzer?

Erlauben ressourcenbasierte Richtlinien den öffentlichen Zugriff?

Sichere Netzwerkkonfiguration

Vermeidet der Service öffentlichen und unsicheren Remote-Netzwerkzugriff?

Verwendet der Service VPCs ordnungsgemäß? Müssen beispielsweise Aufträge in VPCs ausgeführt werden?

Segmentiert und isoliert der Service sensible Ressourcen ordnungsgemäß?

Datenschutz

Verschlüsselung von Daten im Ruhezustand — Verschlüsselt der Dienst Daten im Ruhezustand?

Verschlüsselung von Daten bei der Übertragung — Verschlüsselt der Dienst Daten bei der Übertragung?

Datenintegrität — Validiert der Dienst Daten auf Integrität?

Schutz vor Datenlöschung — Schützt der Dienst Daten vor versehentlichem Löschen?

Datenverwaltung/-nutzung — Verwenden Sie Dienste wie Amazon Macie, um den Standort Ihrer sensiblen Daten zu verfolgen?

API-Schutz

Wird der Service AWS PrivateLink zum Schutz der Service-API-Operationen verwendet?

Schutzdienste

Sind die richtigen Schutzdienste vorhanden? Bieten sie das richtige Maß an Abdeckung?

Schutzdienste helfen Ihnen, Angriffe und Gefährdungen abzuwehren, die auf den Service abzielen. Beispiele für Schutzdienste AWS sind AWS Control Tower,, AWS WAF, Vanta AWS Shield Advanced, Secrets Manager, IAM Access Analyzer und. AWS Resource Access Manager

Sichere Entwicklung

Verwenden Sie sichere Codierungspraktiken?

Vermeiden Sie Schwachstellen wie das Open Web Application Security Project (OWASP) Top Ten?

Detect

Entwickeln und implementieren Sie geeignete Aktivitäten, um das Auftreten eines Cybersicherheitsereignisses zu identifizieren.

Erkennungsservices

Sind die richtigen Erkennungsservices vorhanden?

Bieten sie das richtige Maß an Abdeckung?

Beispiele für AWS Erkennungsdienste sind Amazon GuardDuty AWS Security Hub, Amazon Inspector, Amazon Detective, Amazon CloudWatch Alarms und AWS Trusted Advisor. AWS IoT Device Defender

Reagieren

Entwickeln und implementieren Sie geeignete Aktivitäten, um Maßnahmen in Bezug auf ein erkanntes Cybersicherheitsereignis zu ergreifen.

Reaktionsaktionen

Reagieren Sie schnell auf Sicherheitsereignisse?

Verfügen Sie über aktive Ergebnisse mit kritischem oder hohem Schweregrad?

Forensik

Können Sie sicher forensische Daten für den Service erfassen? Erwerben Sie beispielsweise Amazon EBS-Snapshots, die mit wirklich positiven Ergebnissen verknüpft sind?

Haben Sie ein forensisches Konto eingerichtet?

Wiederherstellung

Entwickeln und implementieren Sie geeignete Aktivitäten, um Ausfallpläne aufrechtzuerhalten und alle Funktionen oder Services wiederherzustellen, die aufgrund eines Cybersicherheitsereignisses beeinträchtigt wurden.

Ausfallsicherheit

Unterstützt die Servicekonfiguration ordnungsgemäße Failovers, elastische Skalierung und hohe Verfügbarkeit?

Haben Sie Sicherungen erstellt?

Aktivierung und Deaktivierung von Steuerungen in allen Standards

AWS Security Hub generiert Ergebnisse für aktivierte Kontrollen und berücksichtigt bei der Berechnung der Sicherheitsbewertungen alle aktivierten Kontrollen. Sie können die Kontrollen für alle Sicherheitsstandards aktivieren und deaktivieren oder den Aktivierungsstatus für

verschiedene Standards unterschiedlich konfigurieren. Wir empfehlen die erstere Option, bei der der Aktivierungsstatus einer Steuerung auf alle aktivierten Standards abgestimmt ist. In diesem Abschnitt wird erklärt, wie Sie Kontrollen standardübergreifend aktivieren und deaktivieren. Informationen zum Aktivieren oder Deaktivieren eines Steuerelements in einem oder mehreren bestimmten Standards finden Sie unterSteuerungen in bestimmten Standards aktivieren und deaktivieren.

Wenn Sie eine Aggregationsregion festgelegt haben, zeigt die Security Hub Hub-Konsole Steuerelemente aus allen verknüpften Regionen an. Wenn ein Steuerelement in einer verknüpften Region verfügbar ist, aber nicht in der Aggregationsregion, können Sie dieses Steuerelement nicht in der Aggregationsregion aktivieren oder deaktivieren.

> **Note**
>
> Die Anweisungen zum Aktivieren und Deaktivieren von Steuerelementen hängen davon ab, ob Sie die zentrale Konfiguration verwenden oder nicht. In diesem Abschnitt werden die Unterschiede beschrieben. Die zentrale Konfiguration steht Benutzern zur Verfügung, die Security Hub und integrieren AWS Organizations. Wir empfehlen, die zentrale Konfiguration zu verwenden, um das Aktivieren und Deaktivieren von Steuerungen in Umgebungen mit mehreren Konten und mehreren Regionen zu vereinfachen.

Steuerungen aktivieren

Wenn Sie ein Steuerelement in einem Standard aktivieren, beginnt Security Hub, Sicherheitsprüfungen für das Steuerelement durchzuführen und Kontrollergebnisse zu generieren.

Security Hub bezieht den Kontrollstatus in die Berechnung der Gesamtsicherheitsbewertung und der Standardsicherheitsbewertungen ein. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erhalten Sie ein einziges Ergebnis für eine Sicherheitsüberprüfung, auch wenn Sie eine Kontrolle in mehreren Standards aktiviert haben. Weitere Informationen finden Sie unter Konsolidierte Erkenntnisse zu Kontrollen.

Aktivierung einer Kontrolle in allen Standards über mehrere Konten und Regionen hinweg

Um eine Sicherheitskontrolle für mehrere Konten und zu aktivieren AWS-Regionen, müssen Sie die zentrale Konfiguration verwenden.

Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte Administrator Security Hub Hub-Konfigurationsrichtlinien erstellen, die bestimmte Kontrollen für alle aktivierten Standards

ermöglichen. Anschließend können Sie die Konfigurationsrichtlinie bestimmten Konten und Organisationseinheiten (OUs) oder dem Stamm zuordnen. Eine Konfigurationsrichtlinie wird in Ihrer Heimatregion (auch Aggregationsregion genannt) und allen verknüpften Regionen wirksam.

Konfigurationsrichtlinien bieten Anpassungsmöglichkeiten. Sie können beispielsweise festlegen, dass alle Steuerelemente in einer Organisationseinheit aktiviert werden, und Sie können festlegen, dass nur Amazon Elastic Compute Cloud (EC2) -Steuerelemente in einer anderen Organisationseinheit aktiviert werden. Der Grad der Granularität hängt von Ihren beabsichtigten Zielen für den Sicherheitsschutz in Ihrem Unternehmen ab. Anweisungen zum Erstellen einer Konfigurationsrichtlinie, die bestimmte Standardkontrollen ermöglicht, finden Sie unterSecurity Hub Hub-Konfigurationsrichtlinien erstellen und zuordnen.

> **Note**
>
> Der delegierte Administrator kann Konfigurationsrichtlinien erstellen, um Kontrollen in allen Standards außer dem Service-Managed Standard zu verwalten:. AWS Control Tower Die Kontrollen für diesen Standard sollten im Service konfiguriert werden. AWS Control Tower

Wenn Sie möchten, dass einige Konten ihre eigenen Steuerungen konfigurieren und nicht der delegierte Administrator, kann der delegierte Administrator diese Konten als selbstverwaltet kennzeichnen. Selbstverwaltete Konten müssen die Kontrollen in jeder Region separat konfigurieren.

Aktivierung einer Steuerung nach allen Standards in einem einzigen Konto und einer einzigen Region

Wenn Sie keine zentrale Konfiguration verwenden oder ein selbstverwaltetes Konto haben, können Sie keine Konfigurationsrichtlinien verwenden, um Steuerungen in mehreren Konten und Regionen zentral zu aktivieren. Sie können jedoch die folgenden Schritte verwenden, um eine Steuerung für ein einzelnes Konto und eine Region zu aktivieren.

Security Hub console

Um eine standardübergreifende Steuerung in einem Konto und einer Region zu ermöglichen

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich die Option Steuerung aus.
3. Wählen Sie die Registerkarte Deaktiviert.

4. Wählen Sie die Option neben einem Steuerelement.
5. Wählen Sie Steuerung aktivieren (diese Option wird nicht für ein Steuerelement angezeigt, das bereits aktiviert ist).
6. Wiederholen Sie den Vorgang in jeder Region, in der Sie das Steuerelement aktivieren möchten.

Security Hub API

Um eine standardübergreifende Steuerung in einem Konto und einer Region zu ermöglichen

1. Rufen Sie die ListStandardsControlAssociationsAPI auf. Geben Sie eine Sicherheitskontroll-ID an.

   Beispiel für eine Anfrage:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. Rufen Sie die BatchUpdateStandardsControlAssociationsAPI auf. Geben Sie den Amazon-Ressourcennamen (ARN) aller Standards an, in denen die Steuerung nicht aktiviert ist. Um Standard-ARNs zu erhalten, führen Sie `DescribeStandards`den Befehl aus.
3. Stellen Sie den `AssociationStatus` Parameter auf`ENABLED`. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits aktiviert ist, gibt die API eine Antwort mit dem HTTP-Statuscode 200 zurück.

   Beispiel für eine Anfrage:

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
   v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
   best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]
   }
   ```

4. Wiederholen Sie dies in jeder Region, in der Sie das Steuerelement aktivieren möchten.

AWS CLI

Um eine standardübergreifende Steuerung in einem Konto und einer Region zu ermöglichen

1. Führen Sie den Befehl list-standards-control-associations aus. Geben Sie eine ID für die Sicherheitskontrolle ein.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Führen Sie den Befehl batch-update-standards-control-associations aus. Geben Sie den Amazon-Ressourcennamen (ARN) aller Standards an, in denen die Steuerung nicht aktiviert ist. Um Standard-ARNs zu erhalten, führen Sie den `describe-standards` Befehl aus.
3. Stellen Sie den `AssociationStatus` Parameter auf`ENABLED`. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits aktiviert ist, gibt der Befehl eine Antwort mit dem HTTP-Statuscode 200 zurück.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0", "AssociationStatus": "ENABLED"}]'
```

4. Wiederholen Sie den Vorgang in jeder Region, in der Sie das Steuerelement aktivieren möchten.

Automatisches Aktivieren neuer Steuerelemente in aktivierten Standards

Security Hub veröffentlicht regelmäßig neue Sicherheitskontrollen und fügt sie zu einem oder mehreren Standards hinzu. Sie können wählen, ob neue Kontrollen in Ihren aktivierten Standards automatisch aktiviert werden sollen.

> **Note**
>
> Wir empfehlen, die zentrale Konfiguration zu verwenden, um neue Steuerungen automatisch zu aktivieren. Wenn Ihre Konfigurationsrichtlinie eine Liste von Steuerelementen enthält, die deaktiviert werden sollen (programmatisch, entspricht dies dem `DisabledSecurityControlIdentifiers` Parameter), aktiviert Security Hub

automatisch alle anderen Kontrollen standardübergreifend, einschließlich neu veröffentlichter Steuerelemente. Wenn Ihre Richtlinie eine Liste der zu aktivierenden Kontrollen enthält (dies entspricht dem `EnabledSecurityControlIdentifiers` Parameter), deaktiviert Security Hub automatisch alle anderen Kontrollen standardübergreifend, auch die neu veröffentlichten. Weitere Informationen finden Sie unter So funktionieren die Security Hub Hub-Konfigurationsrichtlinien.

Wählen Sie Ihre bevorzugte Zugriffsmethode und folgen Sie den Schritten, um neue Kontrollen in aktivierten Standards automatisch zu aktivieren. Die folgenden Anweisungen gelten nur, wenn Sie die zentrale Konfiguration nicht verwenden.

Security Hub console

Um neue Steuerelemente automatisch zu aktivieren

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Einstellungen und dann die Registerkarte Allgemein aus.
3. Wählen Sie unter Steuerelemente die Option Bearbeiten aus.
4. Aktivieren Sie die Option Neue Steuerelemente in aktivierten Standards automatisch aktivieren.
5. Wählen Sie Speichern.

Security Hub API

Um neue Steuerelemente automatisch zu aktivieren

1. Rufen Sie die UpdateSecurityHubConfigurationAPI auf.
2. Um neue Steuerelemente für aktivierte Standards automatisch zu aktivieren, setzen Sie `AutoEnableControls` auf`true`. Wenn Sie neue Steuerelemente nicht automatisch aktivieren möchten, legen Sie den Wert `AutoEnableControls` auf False fest.

AWS CLI

Um neue Steuerelemente automatisch zu aktivieren

1. Führen Sie den Befehl update-security-hub-configuration aus.
2. Um neue Steuerelemente für aktivierte Standards automatisch zu aktivieren, geben Sie an`--auto-enable-controls`. Wenn Sie neue Steuerelemente nicht automatisch aktivieren möchten, geben Sie Folgendes an`--no-auto-enable-controls`.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Beispiel für einen Befehl

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Steuerelemente deaktivieren

Wenn Sie ein Steuerelement in allen Standards deaktivieren, passiert Folgendes:

- Sicherheitsüberprüfungen für das Steuerelement werden nicht mehr durchgeführt.
- Für dieses Steuerelement werden keine zusätzlichen Funde generiert.
- Bestehende Ergebnisse werden automatisch nach 3—5 Tagen archiviert (beachten Sie, dass dies der beste Weg ist).
- Alle zugehörigen AWS Config Regeln, die Security Hub erstellt hat, werden entfernt.

Anstatt ein Steuerelement in allen Standards zu deaktivieren, können Sie es einfach in einem oder mehreren spezifischen Standards deaktivieren. Wenn Sie dies tun, führt Security Hub keine Sicherheitsprüfungen für das Steuerelement für die Standards durch, in denen Sie es deaktiviert haben, sodass sich dies nicht auf die Sicherheitsbewertung dieser Standards auswirkt. Security Hub behält die AWS Config Regel jedoch bei und führt weiterhin Sicherheitsprüfungen für das Steuerelement durch, wenn es in anderen Standards aktiviert ist. Dies kann sich auf Ihre zusammenfassende Sicherheitsbewertung auswirken. Anweisungen zur Konfiguration von Steuerungen in bestimmten Standards finden Sie unterSteuerungen in bestimmten Standards aktivieren und deaktivieren.

Um das Suchgeräusch zu reduzieren, kann es nützlich sein, Steuerungen zu deaktivieren, die für Ihre Umgebung nicht relevant sind. Empfehlungen dazu, welche Steuerelemente Sie deaktivieren sollten, finden Sie unter Security Hub-Steuerelemente, die Sie möglicherweise deaktivieren möchten.

Wenn Sie einen Standard deaktivieren, werden alle Steuerelemente, die für den Standard gelten, deaktiviert (diese Steuerelemente können jedoch in anderen Standards aktiviert bleiben). Informationen zum Deaktivieren eines Standards finden Sie unterthe section called “Aktivieren und Deaktivieren von Standards”.

Wenn Sie einen Standard deaktivieren, verfolgt Security Hub nicht, welche der entsprechenden Kontrollen deaktiviert wurden. Wenn Sie denselben Standard anschließend wieder aktivieren, werden alle für ihn geltenden Kontrollen automatisch aktiviert. Darüber hinaus ist das Deaktivieren eines Steuerelements keine permanente Aktion. Angenommen, Sie deaktivieren ein Steuerelement und aktivieren dann einen Standard, der zuvor deaktiviert war. Wenn der Standard dieses Steuerelement enthält, wird es in diesem Standard aktiviert. Wenn Sie einen Standard in Security Hub aktivieren, werden alle Kontrollen, die für diesen Standard gelten, automatisch aktiviert. Sie können wählen, ob Sie bestimmte Steuerelemente deaktivieren möchten.

Deaktivierung eines Steuerelements in allen Standards für mehrere Konten und Regionen

Um eine Sicherheitskontrolle für mehrere Konten und zu deaktivieren AWS-Regionen, müssen Sie die zentrale Konfiguration verwenden.

Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte Administrator Security Hub Hub-Konfigurationsrichtlinien erstellen, die bestimmte Kontrollen für alle aktivierten Standards deaktivieren. Anschließend können Sie die Konfigurationsrichtlinie bestimmten Konten, Organisationseinheiten oder dem Stammverzeichnis zuordnen. Eine Konfigurationsrichtlinie wird in Ihrer Heimatregion (auch Aggregationsregion genannt) und allen verknüpften Regionen wirksam.

Konfigurationsrichtlinien bieten Anpassungsmöglichkeiten. Sie können beispielsweise festlegen, dass alle AWS CloudTrail Steuerelemente in einer Organisationseinheit und alle IAM-Steuerelemente in einer anderen Organisationseinheit deaktiviert werden. Der Grad der Granularität hängt von Ihren beabsichtigten Zielen für den Sicherheitsschutz in Ihrem Unternehmen ab. Anweisungen zum Erstellen einer Konfigurationsrichtlinie, die bestimmte Kontrollen standardübergreifend deaktiviert, finden Sie unter. Security Hub Hub-Konfigurationsrichtlinien erstellen und zuordnen

> **Note**
>
> Der delegierte Administrator kann Konfigurationsrichtlinien erstellen, um Kontrollen in allen Standards außer dem Service-Managed Standard zu verwalten:. AWS Control Tower Die Kontrollen für diesen Standard sollten im Service konfiguriert werden. AWS Control Tower

Wenn Sie möchten, dass einige Konten ihre eigenen Steuerungen konfigurieren und nicht der delegierte Administrator, kann der delegierte Administrator diese Konten als selbstverwaltet kennzeichnen. Selbstverwaltete Konten müssen die Kontrollen in jeder Region separat konfigurieren.

Deaktivierung einer Steuerung in allen Standards in einem einzigen Konto und einer Region

Wenn Sie keine zentrale Konfiguration verwenden oder ein selbstverwaltetes Konto haben, können Sie keine Konfigurationsrichtlinien verwenden, um Steuerungen in mehreren Konten und Regionen zentral zu deaktivieren. Sie können jedoch die folgenden Schritte verwenden, um eine Steuerung in einem einzelnen Konto und einer Region zu deaktivieren.

Security Hub console

So deaktivieren Sie ein standardübergreifendes Steuerelement in einem Konto und einer Region

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich die Option Steuerung aus.
3. Wählen Sie die Option neben einem Steuerelement aus.
4. Wählen Sie Steuerung deaktivieren (diese Option wird nicht für ein Steuerelement angezeigt, das bereits deaktiviert ist).
5. Wählen Sie einen Grund für die Deaktivierung der Steuerung aus und bestätigen Sie, indem Sie „Deaktivieren“ wählen.
6. Wiederholen Sie den Vorgang in jeder Region, in der Sie das Steuerelement deaktivieren möchten.

Security Hub API

Um ein Steuerelement standardübergreifend in einem Konto und einer Region zu deaktivieren

1. Rufen Sie die ListStandardsControlAssociationsAPI auf. Geben Sie eine Sicherheitskontroll-ID an.

   Beispiel für eine Anfrage:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. Rufen Sie die BatchUpdateStandardsControlAssociationsAPI auf. Geben Sie den ARN aller Standards an, in denen das Steuerelement aktiviert ist. Um Standard-ARNs zu erhalten, führen Sie `DescribeStandards`den Befehl aus.
3. Stellen Sie den `AssociationStatus` Parameter auf`DISABLED`. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits deaktiviert ist, gibt die API eine Antwort mit dem HTTP-Statuscode 200 zurück.

   Beispiel für eine Anfrage:

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-
   benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not
    applicable to environment"}, {"SecurityControlId": "IAM.1", "StandardsArn":
    "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/
   v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
    environment"}}]
   }
   ```

4. Wiederholen Sie dies in jeder Region, in der Sie das Steuerelement deaktivieren möchten.

AWS CLI

Um ein Steuerelement standardübergreifend in einem Konto und einer Region zu deaktivieren

1. Führen Sie den Befehl list-standards-control-associations aus. Geben Sie eine ID für die Sicherheitskontrolle ein.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Führen Sie den Befehl batch-update-standards-control-associations aus. Geben Sie den ARN aller Standards an, in denen das Steuerelement aktiviert ist. Führen Sie den `describe-standards` Befehl aus, um Standard-ARNs zu erhalten.
3. Stellen Sie den `AssociationStatus` Parameter auf`DISABLED`. Wenn Sie diese Schritte für ein Steuerelement ausführen, das bereits deaktiviert ist, gibt der Befehl eine Antwort mit dem HTTP-Statuscode 200 zurück.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable
 to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":
 "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/v/1.4.0",
 "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}]'
```

4. Wiederholen Sie den Vorgang in jeder Region, in der Sie das Steuerelement deaktivieren möchten.

Automatisches Aktivieren neuer Steuerelemente in aktivierten Standards

AWS Security Hub veröffentlicht regelmäßig neue Steuerelemente und fügt sie einem oder mehreren Standards hinzu. Sie können wählen, ob neue Steuerelemente in Ihren aktivierten Standards automatisch aktiviert werden sollen.

> **Note**
>
> Wenn Sie die zentrale Konfiguration verwenden und eine Liste bestimmter Steuerelemente, die deaktiviert werden sollen, in Ihre Konfigurationsrichtlinie aufnehmen (programmatisch, entspricht dies dem `DisabledSecurityControlIdentifiers` Parameter), aktiviert Security Hub automatisch alle anderen Kontrollen standardübergreifend, einschließlich neu veröffentlichter Steuerelemente. Weitere Informationen finden Sie unter So funktionieren die Security Hub Hub-Konfigurationsrichtlinien.

Wir empfehlen, die zentrale Konfiguration von Security Hub zu verwenden, um neue Sicherheitskontrollen automatisch zu aktivieren. Sie können Konfigurationsrichtlinien erstellen, die eine Liste von Steuerelementen enthalten, die standardübergreifend deaktiviert werden sollen. Alle anderen Steuerelemente, einschließlich der neu veröffentlichten, sind standardmäßig aktiviert. Alternativ können Sie Richtlinien erstellen, die eine Liste von Kontrollen enthalten, die standardübergreifend aktiviert werden sollen. Alle anderen Kontrollen, einschließlich der neu veröffentlichten, sind standardmäßig deaktiviert. Weitere Informationen finden Sie unter So funktioniert die zentrale Konfiguration.

Security Hub aktiviert keine neuen Steuerelemente, wenn sie zu einem Standard hinzugefügt werden, den Sie nicht aktiviert haben.

Die folgenden Anweisungen gelten nur, wenn Sie die zentrale Konfiguration nicht verwenden.

Wählen Sie Ihre bevorzugte Zugriffsmethode und folgen Sie den Schritten, um neue Steuerungen in aktivierten Standards automatisch zu aktivieren.

Security Hub console

Um neue Steuerelemente automatisch zu aktivieren

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Einstellungen und dann die Registerkarte Allgemein aus.
3. Wählen Sie unter Steuerelemente die Option Bearbeiten aus.
4. Aktivieren Sie die Option Neue Steuerelemente in aktivierten Standards automatisch aktivieren.
5. Wählen Sie Speichern.

Security Hub API

Um neue Steuerelemente automatisch zu aktivieren

1. Führen Sie `UpdateSecurityHubConfiguration`.
2. Um neue Steuerelemente für aktivierte Standards automatisch zu aktivieren, stellen Sie `AutoEnableControls` auf ein`true`. Wenn Sie neue Steuerelemente nicht automatisch aktivieren möchten, legen Sie den Wert `AutoEnableControls` auf False fest.

AWS CLI

Um neue Steuerelemente automatisch zu aktivieren

1. Führen Sie den Befehl `update-security-hub-configuration` aus.
2. Um neue Steuerelemente für aktivierte Standards automatisch zu aktivieren, geben Sie an `--auto-enable-controls`. Wenn Sie neue Steuerelemente nicht automatisch aktivieren möchten, geben Sie Folgendes an `--no-auto-enable-controls`.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Beispiel für einen Befehl

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Wenn Sie neue Steuerelemente nicht automatisch aktivieren, müssen Sie sie manuell aktivieren. Anweisungen finden Sie unter the section called “Aktivierung und Deaktivierung von Steuerungen in allen Standards”.

Benutzerdefinierte Steuerungsparameter

Einige Security Hub-Steuerelemente verwenden Parameter, die beeinflussen, wie die Steuerung bewertet wird. In der Regel werden solche Kontrollen anhand der von Security Hub definierten Standardparameterwerte bewertet. Für eine Teilmenge dieser Steuerelemente können Sie die Parameterwerte jedoch anpassen. Wenn Sie einen Parameterwert für ein Steuerelement anpassen, beginnt Security Hub, das Steuerelement anhand des von Ihnen angegebenen Werts auszuwerten. Wenn die dem Steuerelement zugrunde liegende Ressource den benutzerdefinierten Wert erfüllt, generiert Security Hub einen `PASSED` Befund. Wenn die Ressource den benutzerdefinierten Wert nicht erfüllt, generiert Security Hub einen `FAILED` Befund.

Durch die Anpassung der Kontrollparameter können Sie die von Security Hub empfohlenen und überwachten bewährten Sicherheitsmethoden verfeinern, um sie an Ihre Geschäftsanforderungen und Sicherheitserwartungen anzupassen. Anstatt die Ergebnisse einer Kontrolle zu unterdrücken, können Sie einen oder mehrere ihrer Parameter anpassen, um Ergebnisse zu erhalten, die Ihren Sicherheitsanforderungen entsprechen.

Im Folgenden finden Sie einige Anwendungsbeispiele für benutzerdefinierte Steuerparameter:

- [CloudWatch.16] — CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden

  Sie können den Aufbewahrungszeitraum angeben.
- [IAM.7] — Passwortrichtlinien für IAM-Benutzer sollten solide Konfigurationen haben

  Sie können Parameter angeben, die sich auf die Passwortstärke beziehen.
- [EC2.18] — Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Verkehr für autorisierte Ports zulassen

  Sie können angeben, welche Ports uneingeschränkten eingehenden Verkehr zulassen dürfen.
- [Lambda.5] — VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren

  Sie können die Mindestanzahl von Availability Zones angeben, die zu einem erfolgreichen Ergebnis führen.

In diesem Abschnitt wird erklärt, wie Sie Steuerparameter anpassen und verwalten.

So funktionieren benutzerdefinierte Steuerparameter

Ein Steuerelement kann einen oder mehrere anpassbare Parameter haben. Zu den möglichen Datentypen für einzelne Steuerparameter gehören die folgenden:

- Boolesch
- Double
- Enum
- EnumList
- Ganzzahl
- IntegerList
- String
- StringList

Bei einigen Steuerelementen müssen akzeptable Parameterwerte ebenfalls in einen bestimmten Bereich fallen, um gültig zu sein. In diesen Fällen bietet Security Hub den akzeptablen Bereich.

Security Hub wählt Standardparameterwerte und aktualisiert sie möglicherweise gelegentlich. Nachdem Sie einen Steuerparameter angepasst haben, entspricht sein Wert weiterhin dem

Wert, den Sie für den Parameter angegeben haben, sofern Sie ihn nicht ändern. Das heißt, der Parameter stoppt die Verfolgung von Aktualisierungen des Security Hub-Standardwerts, auch wenn der benutzerdefinierte Wert des Parameters mit dem aktuellen, von Security Hub definierten Standardwert übereinstimmt. Hier ist ein Beispiel für die Steuerung [ACM.1] — Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 30
            }
        }
    }
}
```

Im vorherigen Beispiel hat der `daysToExpiration` Parameter den benutzerdefinierten Wert. `30` Der aktuelle Standardwert für diesen Parameter ist ebenfalls`30`. Wenn Security Hub den Standardwert auf ändert`14`, verfolgt der Parameter in diesem Beispiel diese Änderung nicht. Er behält den Wert von`30`.

Wenn Sie Aktualisierungen des Security Hub Hub-Standardwerts für einen Parameter verfolgen möchten, setzen Sie das `ValueType` Feld auf `DEFAULT` statt auf`CUSTOM`. Weitere Informationen finden Sie unter Zurücksetzen auf Standardparameterwerte in einem einzigen Konto und einer Region.

Wenn Sie einen Parameterwert ändern, lösen Sie auch eine neue Sicherheitsüberprüfung aus, bei der das Steuerelement anhand des neuen Werts bewertet wird. Security Hub generiert dann neue Kontrollergebnisse auf der Grundlage des neuen Werts. Bei regelmäßigen Updates zur Kontrolle der Ergebnisse verwendet Security Hub auch den neuen Parameterwert. Wenn Sie Parameterwerte für ein Steuerelement ändern, aber keine Standards aktiviert haben, die das Steuerelement enthalten, führt Security Hub keine Sicherheitsprüfungen mit den neuen Werten durch. Sie müssen mindestens einen relevanten Standard für Security Hub aktivieren, um die Steuerung anhand des neuen Parameterwerts auszuwerten.

Benutzerdefinierte Parameterwerte gelten für alle Ihre aktivierten Standards. Sie können die Parameter für ein Steuerelement, das in Ihrer aktuellen Region nicht unterstützt wird, nicht anpassen.

Eine Liste der regionalen Grenzwerte für einzelne Steuerelemente finden Sie unterRegionale Grenzwerte für Kontrollen.

Steuerparameter anpassen

Die Anweisungen zum Anpassen der Steuerparameter variieren je nachdem, ob Sie die zentrale Konfiguration verwenden. Die zentrale Konfiguration ist eine Funktion, mit der der delegierte Security Hub-Administrator die Security Hub Hub-Funktionen für AWS-Regionen Konten und Organisationseinheiten (OUs) in seiner Organisation verwalten kann.

Wenn Ihre Organisation die zentrale Konfiguration verwendet, kann der delegierte Administrator Konfigurationsrichtlinien mit benutzerdefinierten Steuerungsparametern erstellen. Diese Richtlinien können mit zentral verwalteten Mitgliedskonten und Organisationseinheiten verknüpft werden und gelten in Ihrer Heimatregion und allen verknüpften Regionen. Der delegierte Administrator kann auch ein oder mehrere Konten als selbstverwaltete Konten festlegen, sodass der Kontoinhaber seine eigenen Parameter in jeder Region separat konfigurieren kann. Wenn Ihre Organisation keine zentrale Konfiguration verwendet, müssen Sie die Steuerparameter für jedes Konto und jede Region separat anpassen.

Anpassen der Steuerparameter für mehrere Konten und Regionen

Wenn Sie die zentrale Konfiguration verwenden, können Sie die Steuerparameter für zentral verwaltete Konten und Organisationseinheiten über mehrere Konten und Regionen hinweg anpassen. Wir empfehlen, die zentrale Konfiguration zu verwenden, da Sie so die Werte der Steuerparameter in verschiedenen Teilen Ihrer Organisation aufeinander abstimmen können. Beispielsweise könnten alle Ihre Testkonten bestimmte Parameterwerte verwenden, und alle Produktionskonten könnten unterschiedliche Werte verwenden.

Wenn Sie der delegierte Security Hub-Administrator für eine Organisation sind, die die zentrale Konfiguration verwendet, wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um die Steuerungsparameter für mehrere Konten und Regionen anzupassen.

Security Hub console

So passen Sie die Steuerparameter in mehreren Konten und Regionen an

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

   Vergewissern Sie sich, dass Sie in der Heimatregion angemeldet sind.

2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie die Registerkarte Policies.
4. Um eine neue Konfigurationsrichtlinie mit benutzerdefinierten Parametern zu erstellen, wählen Sie Richtlinie erstellen aus. Um benutzerdefinierte Parameter in einer vorhandenen Konfigurationsrichtlinie anzugeben, wählen Sie die Richtlinie aus und klicken Sie dann auf Bearbeiten.

   Um eine neue Konfigurationsrichtlinie mit benutzerdefinierten Parametern zu erstellen

   1. Wählen Sie im Abschnitt Benutzerdefinierte Richtlinie die Sicherheitsstandards und Kontrollen aus, die Sie aktivieren möchten.
   2. Wählen Sie Steuerungsparameter anpassen aus.
   3. Wählen Sie ein Steuerelement aus, und geben Sie dann benutzerdefinierte Werte für einen oder mehrere Parameter an.
   4. Um Parameter für weitere Steuerelemente anzupassen, wählen Sie Zusätzliche Steuerung anpassen.
   5. Wählen Sie im Abschnitt Konten die Konten oder Organisationseinheiten aus, auf die Sie die Richtlinie anwenden möchten.
   6. Wählen Sie Weiter aus.
   7. Wählen Sie Richtlinie erstellen und anwenden aus. In Ihrer Heimatregion und allen verknüpften Regionen setzt diese Aktion die vorhandenen Konfigurationseinstellungen von Konten und Organisationseinheiten außer Kraft, die dieser Konfigurationsrichtlinie zugeordnet sind. Konten und Organisationseinheiten können durch direkte Anwendung oder Vererbung von einem Elternteil mit einer Konfigurationsrichtlinie verknüpft werden.

   Um benutzerdefinierte Parameter in einer vorhandenen Konfigurationsrichtlinie hinzuzufügen oder zu bearbeiten

   1. Geben Sie im Abschnitt Steuerelemente unter Benutzerdefinierte Richtlinie die gewünschten neuen benutzerdefinierten Parameterwerte an.
   2. Wenn Sie in dieser Richtlinie zum ersten Mal Steuerparameter anpassen, wählen Sie Steuerparameter anpassen aus und wählen Sie dann ein Steuerelement aus, das Sie anpassen möchten. Um die Parameter für weitere Steuerelemente anzupassen, wählen Sie Zusätzliche Steuerung anpassen.

3. Überprüfen Sie im Abschnitt Konten die Konten oder Organisationseinheiten, auf die Sie die Richtlinie anwenden möchten.
4. Wählen Sie Weiter aus.
5. Überprüfen Sie Ihre Änderungen und stellen Sie sicher, dass sie korrekt sind. Wenn Sie fertig sind, wählen Sie Richtlinie speichern und anwenden. In Ihrer Heimatregion und allen verknüpften Regionen setzt diese Aktion die vorhandenen Konfigurationseinstellungen von Konten und Organisationseinheiten außer Kraft, die dieser Konfigurationsrichtlinie zugeordnet sind. Konten und Organisationseinheiten können durch direkte Anwendung oder Vererbung von einem Elternteil mit einer Konfigurationsrichtlinie verknüpft werden.

Security Hub API

Um Steuerparameter in mehreren Konten und Regionen anzupassen

Um eine neue Konfigurationsrichtlinie mit benutzerdefinierten Parametern zu erstellen

1. Rufen Sie die CreateConfigurationPolicyAPI über das delegierte Administratorkonto in der Heimatregion auf.
2. Geben Sie für das `SecurityControlCustomParameters` Objekt die ID der einzelnen Steuerelemente an, die Sie anpassen möchten.
3. Geben Sie für das `Parameters` Objekt den Namen jedes Parameters an, den Sie anpassen möchten. Geben Sie für jeden Parameter, den Sie anpassen, Folgendes `CUSTOM` an`ValueType`. Geben Sie für `Value` den Datentyp des Parameters und den benutzerdefinierten Wert an. Das `Value` Feld darf nicht leer sein, wenn `ValueType` es leer ist`CUSTOM`. Wenn Ihre Anfrage einen Parameter auslässt, den das Steuerelement unterstützt, behält dieser Parameter seinen aktuellen Wert bei. Sie können unterstützte Parameter, Datentypen und gültige Werte für ein Steuerelement finden, indem Sie die GetSecurityControlDefinitionAPI aufrufen.

Um benutzerdefinierte Parameter in einer vorhandenen Konfigurationsrichtlinie hinzuzufügen oder zu bearbeiten

1. Rufen Sie die UpdateConfigurationPolicyAPI über das delegierte Administratorkonto in der Heimatregion auf.
2. Geben Sie für das `Identifier` Feld den Amazon-Ressourcennamen (ARN) oder die ID der Konfigurationsrichtlinie ein, die Sie aktualisieren möchten.

3. Geben Sie für das `SecurityControlCustomParameters` Objekt die ID der einzelnen Steuerelemente an, die Sie anpassen möchten.
4. Geben Sie für das `Parameters` Objekt den Namen jedes Parameters an, den Sie anpassen möchten. Geben Sie für jeden Parameter, den Sie anpassen, Folgendes `CUSTOM` an`ValueType`. Geben Sie für `Value` den Datentyp des Parameters und den benutzerdefinierten Wert an. Wenn in Ihrer Anfrage ein Parameter weggelassen wird, den das Steuerelement unterstützt, behält dieser Parameter seinen aktuellen Wert bei. Sie können unterstützte Parameter, Datentypen und gültige Werte für ein Steuerelement finden, indem Sie die GetSecurityControlDefinitionAPI aufrufen.

Beispiel für eine API-Anfrage zum Erstellen einer neuen Konfigurationsrichtlinie:

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"},
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"}
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
```

```
            }
        }
    }
}
```

AWS CLI

Um die Steuerparameter in mehreren Konten und Regionen anzupassen

Um eine neue Konfigurationsrichtlinie mit benutzerdefinierten Parametern zu erstellen

1. Führen Sie den create-configuration-policyBefehl über das delegierte Administratorkonto in der Heimatregion aus.
2. Geben Sie für das `SecurityControlCustomParameters` Objekt die ID der einzelnen Steuerelemente an, die Sie anpassen möchten.
3. Geben Sie für das `Parameters` Objekt den Namen jedes Parameters an, den Sie anpassen möchten. Geben Sie für jeden Parameter, den Sie anpassen, Folgendes `CUSTOM` an`ValueType`. Geben Sie für `Value` den Datentyp des Parameters und den benutzerdefinierten Wert an. Das `Value` Feld darf nicht leer sein, wenn `ValueType` es leer ist`CUSTOM`. Wenn Ihre Anfrage einen Parameter auslässt, den das Steuerelement unterstützt, behält dieser Parameter seinen aktuellen Wert bei. Sie können unterstützte Parameter, Datentypen und gültige Werte für ein Steuerelement finden, indem Sie den get-security-control-definitionBefehl ausführen.

Um Parameter zu einer vorhandenen Konfigurationsrichtlinie hinzuzufügen oder zu bearbeiten

1. Um benutzerdefinierte Eingabeparameter in einer vorhandenen Konfigurationsrichtlinie hinzuzufügen oder zu aktualisieren, führen Sie den update-configuration-policyBefehl über das delegierte Administratorkonto in der Heimatregion aus.
2. Geben Sie für das `identifier` Feld den Amazon-Ressourcennamen (ARN) oder die ID der Richtlinie ein, die Sie aktualisieren möchten.
3. Geben Sie für das `SecurityControlCustomParameters` Objekt die ID jedes Steuerelements an, das Sie anpassen möchten.
4. Geben Sie für das `Parameters` Objekt den Namen jedes Parameters an, den Sie anpassen möchten. Geben Sie für jeden Parameter, den Sie anpassen, Folgendes `CUSTOM` an`ValueType`. Geben Sie für `Value` den Datentyp des Parameters und den benutzerdefinierten Wert an. Wenn in Ihrer Anfrage ein Parameter weggelassen wird, den

das Steuerelement unterstützt, behält dieser Parameter seinen aktuellen Wert bei. Sie können unterstützte Parameter, Datentypen und gültige Werte für ein Steuerelement finden, indem Sie den get-security-control-definitionBefehl ausführen.

Beispielbefehl zum Erstellen einer neuen Konfigurationsrichtlinie:

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": "Integer": 15}}}]}}}'
```

Anpassen der Steuerparameter in einem einzigen Konto und einer Region

Wenn Sie keine zentrale Konfiguration verwenden oder kein selbstverwaltetes Konto haben, können Sie die Steuerparameter für Ihr Konto jeweils in einer Region anpassen

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zur Anpassung der Steuerparameter. Ihre Änderungen gelten nur für Ihr Konto in der aktuellen Region. Um die Steuerungsparameter in weiteren Regionen anzupassen, wiederholen Sie die folgenden Schritte für jedes weitere Konto und jede Region, in der Sie die Parameter anpassen möchten. Das gleiche Steuerelement kann in verschiedenen Regionen unterschiedliche Parameterwerte verwenden.

Security Hub console

Um Steuerparameter in einem Konto und einer Region anzupassen

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Controls aus. Wählen Sie in der Tabelle ein Steuerelement aus, das benutzerdefinierte Parameter unterstützt und für das Sie die Parameter

ändern möchten. In der Spalte Benutzerdefinierte Parameter wird angegeben, welche Steuerelemente benutzerdefinierte Parameter unterstützen.

3. Wählen Sie auf der Detailseite für das Steuerelement die Registerkarte Parameter und dann Bearbeiten aus.
4. Geben Sie die gewünschten Parameterwerte an.
5. Wählen Sie optional im Abschnitt Grund für die Änderung einen Grund für die Anpassung der Parameter aus.
6. Wählen Sie Speichern.

Security Hub API

Um die Steuerparameter in einem Konto und einer Region anzupassen

1. Rufen Sie die UpdateSecurityControlAPI auf.
2. Geben Sie für `SecurityControlId` die ID des Steuerelements an, das Sie anpassen möchten.
3. Geben Sie für das `Parameters` Objekt den Namen jedes Parameters an, den Sie anpassen möchten. Geben Sie für jeden Parameter, den Sie anpassen, Folgendes `CUSTOM` an`ValueType`. Geben Sie für `Value` den Datentyp des Parameters und den benutzerdefinierten Wert an. Wenn in Ihrer Anfrage ein Parameter weggelassen wird, den das Steuerelement unterstützt, behält dieser Parameter seinen aktuellen Wert bei. Sie können unterstützte Parameter, Datentypen und gültige Werte für ein Steuerelement finden, indem Sie die GetSecurityControlDefinitionAPI aufrufen.
4. Geben Sie optional für `LastUpdateReason` einen Grund für die Anpassung der Steuerparameter an.

Beispiel für eine API-Anfrage:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 15
            }
```

```
        }
    },
    "LastUpdateReason": "Internal compliance requirement"
}
```

AWS CLI

Um die Steuerparameter in einem Konto und einer Region anzupassen

1. Führen Sie den Befehl update-security-control aus.
2. Geben Sie für `security-control-id` die ID des Steuerelements an, das Sie anpassen möchten.
3. Geben Sie für das `parameters` Objekt den Namen jedes Parameters an, den Sie anpassen möchten. Geben Sie für jeden Parameter, den Sie anpassen, Folgendes `CUSTOM` an`ValueType`. Geben Sie für `Value` den Datentyp des Parameters und den benutzerdefinierten Wert an. Wenn in Ihrer Anfrage ein Parameter weggelassen wird, den das Steuerelement unterstützt, behält dieser Parameter seinen aktuellen Wert bei. Sie können unterstützte Parameter, Datentypen und gültige Werte für ein Steuerelement finden, indem Sie den get-security-control-definitionBefehl ausführen.
4. Geben Sie optional für `last-update-reason` einen Grund für die Anpassung der Steuerparameter an.

Beispielbefehl:

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":
 15}}}' \
--last-update-reason "Internal compliance requirement"
```

Überprüfen des Status der Steuerparameter

Es ist wichtig, den Status von Änderungen an den Steuerparametern zu validieren und zu überprüfen. Auf diese Weise wird sichergestellt, dass eine Kontrolle erwartungsgemäß funktioniert und den beabsichtigten Sicherheitswert bietet. Um zu überprüfen, ob ein Parameter-Update erfolgreich war, können Sie die Details der Steuerung auf der Security Hub Hub-Konsole überprüfen. Wählen Sie auf

der Konsole das Steuerelement aus, dessen Details angezeigt werden sollen. Auf der Registerkarte Parameter wird der Status der Parameteränderung angezeigt.

Wenn Ihre Anfrage zur Aktualisierung eines Parameters gültig ist, ist der Wert des `UpdateStatus` Felds programmgesteuert eine Antwort auf den BatchGetSecurityControlsVorgang. `UPDATING` Das bedeutet, dass die Aktualisierung gültig war, Ihre Ergebnisse jedoch möglicherweise noch nicht die aktualisierten Parameterwerte enthalten. Wenn sich der Wert von `UpdateState` ändert`READY`, beginnen Ihre Ergebnisse, die aktualisierten Parameterwerte zu enthalten.

Der `UpdateSecurityControl` Vorgang gibt eine `InvalidInputException` Antwort für ungültige Parameterwerte zurück. Die Antwort enthält zusätzliche Details zur Ursache des Fehlers. Beispielsweise haben Sie möglicherweise einen Wert angegeben, der außerhalb des gültigen Bereichs für einen Parameter liegt. Oder Sie haben einen Wert angegeben, der nicht den richtigen Datentyp verwendet. Senden Sie Ihre Anfrage erneut mit einer gültigen Eingabe. Wenn ein Parameter-Update nicht erfolgreich ist, behält Security Hub den aktuellen Wert für den Parameter bei.

Wenn beim Versuch, einen Parameterwert zu aktualisieren, ein interner Fehler auftritt, versucht Security Hub es automatisch erneut, sofern Sie AWS Config es aktiviert haben. Weitere Informationen finden Sie unter Konfiguration AWS Config.

Überprüfung der Steuerparameter

Sie können die aktuellen Werte für einzelne Steuerparameter in Ihrem Konto überprüfen. Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte Security Hub-Administrator auch Parameterwerte überprüfen, die in einer Konfigurationsrichtlinie angegeben sind.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um die aktuellen Steuerparameterwerte zu überprüfen.

Security Hub console

Um die aktuellen Parameterwerte zu überprüfen

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Controls aus. Wählen Sie ein Steuerelement aus.
3. Wählen Sie die Registerkarte Parameters aus. Auf dieser Registerkarte werden die aktuellen Parameterwerte für das Steuerelement angezeigt.

Security Hub API

Um die aktuellen Parameterwerte zu überprüfen

Rufen Sie die BatchGetSecurityControlsAPI auf und geben Sie eine oder mehrere Sicherheitskontroll-IDs oder ARNs an. Das `Parameters` Objekt in der Antwort zeigt die aktuellen Parameterwerte für die angegebenen Steuerelemente.

Beispiel für eine API-Anfrage:

```
{
    "SecurityControlIds": ["APIGateway.1", "CloudWatch.15", "IAM.7"]
}
```

AWS CLI

Um aktuelle Parameterwerte zu überprüfen

Führen Sie den batch-get-security-controlsBefehl aus und geben Sie eine oder mehrere Sicherheitskontroll-IDs oder ARNs ein. Das `Parameters` Objekt in der Antwort zeigt die aktuellen Parameterwerte für die angegebenen Steuerelemente an.

Beispielbefehl:

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

Wählen Sie Ihre bevorzugte Methode, um die aktuellen Parameterwerte in einer zentralen Konfigurationsrichtlinie anzuzeigen.

Security Hub console

Um aktuelle Parameterwerte in einer Konfigurationsrichtlinie zu überprüfen

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub-Administratorkontos in der Heimatregion an.

2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie auf der Registerkarte Richtlinien die Konfigurationsrichtlinie aus und klicken Sie dann auf Details anzeigen. Anschließend werden die Richtliniendetails angezeigt, einschließlich der aktuellen Parameterwerte.

Security Hub API

Um aktuelle Parameterwerte in einer Konfigurationsrichtlinie zu überprüfen

1. Rufen Sie die GetConfigurationPolicyAPI über das delegierte Administratorkonto in der Heimatregion auf.
2. Geben Sie den ARN oder die ID der Konfigurationsrichtlinie an, deren Details Sie sehen möchten. Die Antwort enthält aktuelle Parameterwerte.

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

Um aktuelle Parameterwerte in einer Konfigurationsrichtlinie zu überprüfen

1. Führen Sie den get-configuration-policyBefehl über das delegierte Administratorkonto in der Heimatregion aus.
2. Geben Sie den ARN oder die ID der Konfigurationsrichtlinie an, deren Details Sie sehen möchten. Die Antwort enthält aktuelle Parameterwerte.

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Ihre Kontrollergebnisse zeigen auch aktuelle Parameterwerte. In der AWS Syntax des Security Finding Format (ASFF) erscheinen diese Werte im `Parameters` Feld des `Compliance` Objekts. Um die Ergebnisse auf der Security Hub Hub-Konsole zu überprüfen, wählen Sie im Navigationsbereich Findings aus. Verwenden Sie den Vorgang, um die Ergebnisse programmgesteuert zu überprüfen. GetFindings

> **Note**
>
> Nach der Veröffentlichung der Funktion für benutzerdefinierte Steuerparameter aktualisiert Security Hub die vorhandenen Kontrollergebnisse, um das `Parameters` ASFF-Feld einzubeziehen. Dies kann bis zu 24 Stunden dauern.

Rückkehr zu den Standardwerten der Steuerparameter

Ein Steuerparameter kann einen Standardwert haben, den Security Hub definiert. Möglicherweise aktualisieren wir den Standardwert für einen Parameter, um den sich entwickelnden bewährten Sicherheitsmethoden Rechnung zu tragen. Wenn Sie keinen benutzerdefinierten Wert für einen Steuerparameter angegeben haben, verfolgt das Steuerelement diese Aktualisierungen automatisch und verwendet den neuen Standardwert.

Sie können zur Verwendung der Standardparameterwerte für ein Steuerelement zurückkehren. Wie Sie das tun, hängt davon ab, ob Sie die zentrale Konfiguration verwenden.

> **Note**
>
> Nicht alle Steuerparameter haben einen Security Hub Hub-Standardwert. In solchen Fällen, wenn auf gesetzt `ValueType` ist`DEFAULT`, gibt es keinen bestimmten Standardwert, den Security Hub verwendet. Stattdessen ignoriert Security Hub den Parameter, wenn kein benutzerdefinierter Wert vorhanden ist.

Zurücksetzen auf Standardparameterwerte für mehrere Konten und Regionen

Wenn Sie die zentrale Konfiguration verwenden, können Sie die Steuerparameter für zentral verwaltete Konten und Organisationseinheiten über mehrere Konten und Regionen hinweg zurücksetzen.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um mithilfe der zentralen Konfiguration zu den Standardparameterwerten für mehrere Konten und Regionen zurückzukehren.

Security Hub console

So kehren Sie in mehreren Konten und Regionen zu den Standardparameterwerten zurück

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.

   Melden Sie sich mit den Anmeldeinformationen des delegierten Security Hub-Administratorkontos in der Heimatregion an.
2. Wählen Sie im Navigationsbereich Einstellungen und Konfiguration aus.
3. Wählen Sie die Registerkarte Policies.
4. Wählen Sie eine Richtlinie aus und klicken Sie dann auf Bearbeiten.
5. Unter Benutzerdefinierte Richtlinie wird im Abschnitt Steuerelemente eine Liste der Steuerelemente angezeigt, für die Sie benutzerdefinierte Parameter angegeben haben.
6. Suchen Sie das Steuerelement mit einem oder mehreren Parameterwerten, die rückgängig gemacht werden sollen. Wählen Sie dann Entfernen, um zu den Standardwerten zurückzukehren.
7. Überprüfen Sie im Abschnitt Konten die Konten oder Organisationseinheiten, auf die Sie die Richtlinie anwenden möchten.
8. Wählen Sie Weiter aus.
9. Überprüfen Sie Ihre Änderungen und stellen Sie sicher, dass sie korrekt sind. Wenn Sie fertig sind, wählen Sie Richtlinie speichern und anwenden. In Ihrer Heimatregion und allen verknüpften Regionen setzt diese Aktion die vorhandenen Konfigurationseinstellungen von Konten und Organisationseinheiten außer Kraft, die dieser Konfigurationsrichtlinie zugeordnet sind. Konten und Organisationseinheiten können durch direkte Anwendung oder Vererbung von einem Elternteil mit einer Konfigurationsrichtlinie verknüpft werden.

Security Hub API

Um in mehreren Konten und Regionen zu den Standardparameterwerten zurückzukehren

1. Rufen Sie die UpdateConfigurationPolicyAPI vom delegierten Administratorkonto in der Heimatregion aus auf.

2. Geben Sie für das `Identifier` Feld den Amazon-Ressourcennamen (ARN) oder die ID der Richtlinie ein, die Sie aktualisieren möchten.
3. Geben Sie für das `SecurityControlCustomParameters` Objekt die ID jedes Steuerelements an, für das Sie einen oder mehrere Parameter rückgängig machen möchten.
4. Geben Sie im `Parameters` Objekt für jeden Parameter, den Sie rückgängig machen möchten, das `ValueType` Feld `DEFAULT` an. Wenn auf gesetzt `ValueType` ist`DEFAULT`, müssen Sie keinen Wert für das `Value` Feld angeben. Wenn in Ihrer Anfrage ein Wert enthalten ist, ignoriert Security Hub ihn. Wenn in Ihrer Anfrage ein Parameter weggelassen wird, den das Steuerelement unterstützt, behält dieser Parameter seinen aktuellen Wert bei.

> **Warning**
>
> Wenn Sie ein Kontrollobjekt aus dem `SecurityControlCustomParameters` Feld weglassen, setzt Security Hub alle benutzerdefinierten Parameter für das Steuerelement auf ihre Standardwerte zurück. Eine völlig leere Liste für `SecurityControlCustomParameters` setzt benutzerdefinierte Parameter für alle Steuerelemente auf ihre Standardwerte zurück.

Beispiel für eine API-Anfrage:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "TestConfigurationPolicy",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Revert ACM.1 parameter to default value",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"},
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"}
                ],
             "SecurityControlsConfiguration": {
                "DisbledSecurityControlIdentifiers": [
                    "CloudTrail.2"
```

```
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "DEFAULT"
                             }
                         }
                    }
                ]
            }
        }
    }
}
```

AWS CLI

Um zu den Standardparameterwerten in mehreren Konten und Regionen zurückzukehren

1. Führen Sie den update-configuration-policyBefehl über das delegierte Administratorkonto in der Heimatregion aus.
2. Geben Sie für das `identifier` Feld den Amazon-Ressourcennamen (ARN) oder die ID der Richtlinie ein, die Sie aktualisieren möchten.
3. Geben Sie für das `SecurityControlCustomParameters` Objekt die ID jedes Steuerelements an, für das Sie einen oder mehrere Parameter rückgängig machen möchten.
4. Geben Sie im `Parameters` Objekt für jeden Parameter, den Sie rückgängig machen möchten, das `ValueType` Feld `DEFAULT` an. Wenn auf gesetzt `ValueType` ist`DEFAULT`, müssen Sie keinen Wert für das `Value` Feld angeben. Wenn in Ihrer Anfrage ein Wert enthalten ist, ignoriert Security Hub ihn. Wenn in Ihrer Anfrage ein Parameter weggelassen wird, den das Steuerelement unterstützt, behält dieser Parameter seinen aktuellen Wert bei.

> **Warning**
>
> Wenn Sie ein Kontrollobjekt aus dem `SecurityControlCustomParameters` Feld weglassen, setzt Security Hub alle benutzerdefinierten Parameter für das Steuerelement auf ihre Standardwerte zurück. Eine völlig leere Liste für

`SecurityControlCustomParameters` setzt benutzerdefinierte Parameter für alle Steuerelemente auf ihre Standardwerte zurück.

Beispielbefehl:

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--name "TestConfigurationPolicy" \
--description "Updated configuration policy" \
--updated-reason "Revert ACM.1 parameter to default value"
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "DEFAULT"}}}]}}'
```

Zurücksetzen auf Standardparameterwerte in einem einzigen Konto und einer Region

Wenn Sie keine zentrale Konfiguration verwenden oder über ein selbstverwaltetes Konto verfügen, können Sie für Ihr Konto in jeweils einer Region wieder die Standardparameterwerte verwenden.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten, um zu den Standardparameterwerten für Ihr Konto in einer einzelnen Region zurückzukehren. Um in weiteren Regionen zu den Standardparameterwerten zurückzukehren, wiederholen Sie diese Schritte in jeder weiteren Region.

Note

Wenn Sie Security Hub deaktivieren, werden Ihre benutzerdefinierten Steuerungsparameter zurückgesetzt. Wenn Sie Security Hub in future erneut aktivieren, verwenden alle Steuerelemente beim Start Standardparameterwerte.

Security Hub console

Um zu den Standardparameterwerten in einem Konto und einer Region zurückzukehren

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Controls aus. Wählen Sie das Steuerelement aus, für das Sie die Standardparameterwerte wiederherstellen möchten.
3. Wählen Sie auf der **Parameters** Registerkarte neben einem Steuerparameter die Option Benutzerdefiniert aus. Wählen Sie dann Anpassung entfernen aus. Dieser Parameter verwendet jetzt den Security Hub Hub-Standardwert und verfolgt future Updates auf den Standardwert.
4. Wiederholen Sie den vorherigen Schritt für jeden Parameterwert, den Sie wiederherstellen möchten.

Security Hub API

Um zu den Standardparameterwerten in einem Konto und einer Region zurückzukehren

1. Rufen Sie die API auf UpdateSecurityControl.
2. Geben Sie für `SecurityControlId` den ARN oder die ID des Steuerelements an, dessen Parameter Sie rückgängig machen möchten.
3. Geben Sie im `Parameters` Objekt für jeden Parameter, den Sie rückgängig machen möchten, das `ValueType` Feld `DEFAULT` an. Wenn auf gesetzt `ValueType` ist`DEFAULT`, müssen Sie keinen Wert für das `Value` Feld angeben. Wenn in Ihrer Anfrage ein Wert enthalten ist, ignoriert Security Hub ihn.
4. Geben Sie optional einen Grund für `LastUpdateReason` die Rückkehr zu den Standardparameterwerten an.

Beispiel für eine API-Anfrage:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "DEFAULT"
        },
```

```
    "LastUpdateReason": "New internal requirement"
}
```

AWS CLI

Um zu den Standardparameterwerten in einem Konto und einer Region zurückzukehren

1. Führen Sie den Befehl update-security-control aus.
2. Geben Sie für `security-control-id` den ARN oder die ID des Steuerelements an, dessen Parameter Sie rückgängig machen möchten.
3. Geben Sie im `parameters` Objekt für jeden Parameter, den Sie rückgängig machen möchten, das `ValueType` Feld `DEFAULT` an. Wenn auf gesetzt `ValueType` ist`DEFAULT`, müssen Sie keinen Wert für das `Value` Feld angeben. Wenn in Ihrer Anfrage ein Wert enthalten ist, ignoriert Security Hub ihn.
4. Geben Sie optional einen Grund für `last-update-reason` die Rückkehr zu den Standardparameterwerten an.

Beispielbefehl:

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

Steuerelemente, die benutzerdefinierte Parameter unterstützen

Eine Liste der Sicherheitskontrollen, die benutzerdefinierte Parameter unterstützen, finden Sie auf der Seite Steuerungen in der Security Hub Hub-Konsole oder imReferenz zu Security Hub-Steuerungen. Um diese Liste programmgesteuert abzurufen, können Sie den ListSecurityControlDefinitionsVorgang verwenden. In der Antwort gibt das `CustomizableProperties` Objekt an, welche Steuerelemente anpassbare Parameter unterstützen.

Security Hub-Steuerelemente, die Sie möglicherweise deaktivieren möchten

Wir empfehlen, einige AWS Security Hub Steuerungen zu deaktivieren, um den Suchlärm zu reduzieren und die Kosten zu begrenzen.

Kontrollen, die sich mit globalen Ressourcen befassen

Einige AWS-Services unterstützen globale Ressourcen, was bedeutet, dass Sie von jeder Ressource aus auf die Ressource zugreifen können AWS-Region. Um Kosten zu sparen AWS Config, können Sie die Aufzeichnung globaler Ressourcen in allen Regionen außer einer Region deaktivieren. Nachdem Sie dies getan haben, führt Security Hub jedoch weiterhin Sicherheitsüberprüfungen in allen Regionen durch, in denen eine Kontrolle aktiviert ist, und berechnet Ihnen Gebühren auf der Grundlage der Anzahl der Prüfungen pro Konto pro Region. Um das Suchgeräusch zu reduzieren und die Kosten für Security Hub zu senken, sollten Sie daher auch Kontrollen deaktivieren, die globale Ressourcen in allen Regionen betreffen, mit Ausnahme der Region, in der globale Ressourcen erfasst werden.

Wenn ein Steuerelement globale Ressourcen umfasst, aber nur in einer Region verfügbar ist, können Sie, wenn Sie es in dieser Region deaktivieren, keine Ergebnisse für die zugrunde liegende Ressource abrufen. In diesem Fall empfehlen wir, das Steuerelement aktiviert zu lassen. Wenn Sie die regionsübergreifende Aggregation verwenden, sollte die Region, in der das Steuerelement verfügbar ist, die Aggregationsregion oder eine der verknüpften Regionen sein. Die folgenden Steuerelemente beziehen sich auf globale Ressourcen, sind jedoch nur in einer einzigen Region verfügbar:

- Alle CloudFront Steuerelemente — Nur in USA Ost (Nord-Virginia) verfügbar
- GlobalAccelerator.1 — Nur in den USA West (Oregon) verfügbar
- Route 53.2 — Nur in den USA Ost (Nord-Virginia) verfügbar
- WAF.1, WAF.6, WAF.7 und WAF.8 — Nur in den USA Ost (Nord-Virginia) verfügbar

> **Note**
>
> Wenn Sie die zentrale Konfiguration verwenden, deaktiviert Security Hub automatisch Steuerungen, die globale Ressourcen in allen Regionen außer der Heimatregion betreffen. Andere Steuerelemente, die Sie über eine Konfigurationsrichtlinie aktivieren, sind in allen Regionen aktiviert, in denen sie verfügbar sind. Um die Ergebnisse für diese Steuerelemente auf nur eine Region zu beschränken, können Sie Ihre AWS Config Rekordereinstellungen aktualisieren und die globale Ressourcenaufzeichnung in allen Regionen außer der Heimatregion deaktivieren. Wenn Sie die zentrale Konfiguration verwenden, fehlt Ihnen die Abdeckung für ein Steuerelement, das in der Heimatregion und einer der verknüpften

Regionen nicht verfügbar ist. Weitere Informationen zur zentralen Konfiguration finden Sie unterSo funktioniert die zentrale Konfiguration.

Wenn Sie die Aufzeichnung globaler Ressourcen in einer oder mehreren Regionen deaktivieren, generiert das Steuerelement [Config.1] AWS Config sollte aktiviert sein, in diesen Regionen ein fehlgeschlagenes Ergebnis. Dies liegt daran, dass Config.1 die Aufzeichnung globaler Ressourcen erfordert, um erfolgreich zu sein. Sie können die Ergebnisse für dieses Steuerelement manuell oder mithilfe einer Automatisierungsregel unterdrücken.

Bei Kontrollen mit einem periodischen Zeitplan ist es erforderlich, sie in Security Hub zu deaktivieren, um eine Abrechnung zu verhindern. Die Einstellung des AWS Config Parameters `includeGlobalResourceTypes` auf `false` hat keinen Einfluss auf regelmäßige Security Hub-Steuerungen.

Im Folgenden finden Sie eine Liste der Security Hub-Steuerelemente, die globale Ressourcen betreffen:

- [Account.1] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto
- [Account.2] AWS-Konten sollte Teil einer Organisation sein AWS Organizations
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen

- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen
- [IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.
- [IAM.7] Die Passwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.10] Passwortrichtlinien für IAM-Benutzer sollten strenge Laufzeiten haben AWS Config
- [IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert
- [IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert
- [IAM.13] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist
- [IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert
- [IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
- [IAM.16] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert
- [IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen

- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein

Kontrollen, die sich mit der CloudTrail Protokollierung befassen

Dieses Steuerelement befasst sich mit der Verwendung von AWS Key Management Service (AWS KMS) zur Verschlüsselung von AWS CloudTrail Trail-Logs. Wenn Sie diese Pfade in einem zentralen Protokollierungskonto protokollieren, müssen Sie diese Steuerung nur in dem Konto und der Region aktivieren, in der die zentrale Protokollierung stattfindet.

> **Note**
>
> Wenn Sie die zentrale Konfiguration verwenden, wird der Aktivierungsstatus eines Steuerelements auf die Heimatregion und die verknüpften Regionen verteilt. Sie können

ein Steuerelement nicht in einigen Regionen deaktivieren und in anderen aktivieren. Unterdrücken Sie in diesem Fall die Ergebnisse der folgenden Steuerelemente, um das Suchrauschen zu reduzieren.

- [CloudTrail.2] CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben

Steuerungen, die sich mit CloudWatch Alarmen befassen

Wenn Sie Amazon GuardDuty für die Erkennung von Anomalien anstelle von CloudWatch Amazon-Alarmen bevorzugen, können Sie diese Steuerungen deaktivieren, die sich auf CloudWatch Alarme konzentrieren.

- [CloudWatch.1] Für den Benutzer „root“ sollten ein Metrik-Logfilter und ein Alarm vorhanden sein
- [CloudWatch.2] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind
- [CloudWatch.3] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Anmeldung an der Management Console ohne MFA vorhanden sind
- [CloudWatch.4] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für IAM-Richtlinienänderungen vorhanden sind
- [CloudWatch1.5] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen der Dauer CloudTrail AWS Config vorhanden sind
- [CloudWatch.6] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Management Console Authentifizierungsfehler vorhanden sind
- [CloudWatch.7] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Deaktivierung oder das geplante Löschen von vom Kunden verwalteten Schlüsseln vorhanden sind
- [CloudWatch.8] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind
- [CloudWatch.9] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Config Konfigurationsänderungen vorhanden sind
- [CloudWatch.10] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Sicherheitsgruppen vorhanden sind
- [CloudWatch.11] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind

- [CloudWatch.12] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an Netzwerk-Gateways vorhanden sind
- [CloudWatch.13] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Änderungen an der Routentabelle vorhanden sind
- [CloudWatch.14] Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für VPC-Änderungen vorhanden sind

Details für ein Steuerelement anzeigen

Für jede AWS Security Hub Kontrolle können Sie eine Seite mit nützlichen Details anzeigen.

Oben auf der Seite mit den Kontrolldetails finden Sie einen Überblick über das Steuerelement, einschließlich:

- Aktivierungsstatus — Oben auf der Seite erfahren Sie, ob die Steuerung für mindestens einen Standard in mindestens einem Mitgliedskonto aktiviert ist. Wenn Sie eine Aggregationsregion festgelegt haben, ist das Steuerelement aktiviert, wenn es für mindestens einen Standard in mindestens einer Region aktiviert ist. Wenn das Steuerelement deaktiviert ist, können Sie es von dieser Seite aus aktivieren. Wenn das Steuerelement aktiviert ist, können Sie es auf dieser Seite deaktivieren. Weitere Informationen finden Sie unter the section called “Aktivierung und Deaktivierung von Steuerungen in allen Standards”.
- Kontrollstatus — Dieser Status fasst die Leistung einer Kontrolle auf der Grundlage des Konformitätsstatus der Kontrollergebnisse zusammen. Security Hub generiert den anfänglichen Kontrollstatus in der Regel innerhalb von 30 Minuten nach Ihrem ersten Besuch der Übersichtsseite oder der Seite Sicherheitsstandards in der Security Hub Hub-Konsole. Status sind nur für Kontrollen verfügbar, die aktiviert werden, wenn Sie diese Seiten besuchen. Verwenden Sie den `UpdateStandardsControl`API-Vorgang, um ein Steuerelement zu aktivieren oder zu deaktivieren. Darüber hinaus muss die AWS Config Ressourcenaufzeichnung konfiguriert sein, damit der Kontrollstatus angezeigt wird. Nachdem der Kontrollstatus zum ersten Mal generiert wurde, aktualisiert Security Hub den Kontrollstatus alle 24 Stunden auf der Grundlage der Ergebnisse der letzten 24 Stunden. Auf der Standarddetailseite und der Kontrolldetailseite zeigt Security Hub einen Zeitstempel an, der angibt, wann der Status zuletzt aktualisiert wurde.

  Für Administratorkonten wird ein aggregierter Kontrollstatus für das Administratorkonto und die Mitgliedskonten angezeigt. Wenn Sie eine Aggregationsregion festgelegt haben, umfasst der Kontrollstatus Ergebnisse aus allen verknüpften Regionen. Weitere Informationen zum Kontrollstatus finden Sie unterthe section called “Konformitätsstatus und Kontrollstatus”.

> **Note**
>
> Nach der Aktivierung eines Steuerelements kann es bis zu 24 Stunden dauern, bis in den Regionen China und erstmalige Kontrollstatus generiert werden. AWS GovCloud (US) Region

Auf der Registerkarte Standards und Anforderungen sind die Standards aufgeführt, für die eine Kontrolle aktiviert werden kann, sowie die Anforderungen, die sich aus den verschiedenen Compliance-Frameworks ergeben, in Bezug auf die Kontrolle.

Unten auf der Detailseite finden Sie Informationen zu den aktiven Ergebnissen der Kontrolle. Die Ergebnisse der Kontrolle werden durch Sicherheitsüberprüfungen anhand der Kontrolle generiert. Die Liste der Kontrollergebnisse enthält keine archivierten Ergebnisse.

Die Ergebnisliste verwendet Registerkarten, auf denen verschiedene Teilmengen der Liste angezeigt werden. Auf den meisten Registerkarten werden in der Ergebnisliste Ergebnisse angezeigt, die den Workflow-Status `NEWNOTIFIED`, oder `RESOLVED` haben. Auf einer separaten Registerkarte werden `SUPPRESSED` Ergebnisse angezeigt.

Für jedes Ergebnis bietet die Liste Zugriff auf Ergebnisdetails wie den Konformitätsstatus und die zugehörige Ressource. Sie können auch den Workflow-Status für jedes Ergebnis festlegen und Ergebnisse an benutzerdefinierte Aktionen senden. Weitere Informationen finden Sie unter the section called “Kontrollergebnisse anzeigen und entsprechende Maßnahmen ergreifen”.

Details für ein Steuerelement anzeigen

Wählen Sie Ihre bevorzugte Zugriffsmethode und gehen Sie wie folgt vor, um Details zu einem Steuerelement anzuzeigen. Die Details beziehen sich auf das Girokonto und die Region und beinhalten Folgendes:

- Titel und Beschreibung der Kontrolle
- Link zu Anweisungen zur Behebung fehlgeschlagener Kontrollergebnisse
- Schweregrad der Kontrolle
- Aktivierungsstatus der Kontrolle
- (Auf der Konsole) Eine Liste der aktuellen Ergebnisse für das Steuerelement. Verwenden Sie bei Verwendung der Security Hub Hub-API oder AWS CLI`GetFindings`zum Abrufen von Kontrollergebnissen.

Security Hub console

1. Öffnen Sie die AWS Security Hub Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Controls aus.
3. Wählen Sie ein Steuerelement aus.

Security Hub API

1. Führen Sie `ListSecurityControlDefinitions` einen oder mehrere Standard-ARNs aus und geben Sie ihn an, um eine Liste der Kontroll-IDs für diesen Standard zu erhalten. Um Standard-ARNs zu erhalten, führen Sie den Befehl aus. `DescribeStandards` Wenn Sie keinen Standard-ARN angeben, gibt diese API alle Security Hub-Steuerungs-IDs zurück. Diese API gibt standardunabhängige Sicherheitskontroll-IDs zurück, nicht die standardbasierten Kontroll-IDs, die vor diesen Feature-Releases existierten.

   Beispiel für eine Anfrage:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Ausführen`BatchGetSecurityControls`, um Details zu einem oder mehreren Steuerelementen im aktuellen AWS-Konto und abzurufen AWS-Region.

   Beispiel für eine Anfrage:

   ```
   {
       "SecurityControlIds": ["Config.1", "IAM.1"]
   }
   ```

AWS CLI

1. Führen Sie den `list-security-control-definitions` Befehl aus und geben Sie einen oder mehrere Standard-ARNs an, um eine Liste von Kontroll-IDs zu erhalten. Führen Sie den Befehl aus, um Standard-ARNs zu erhalten. `describe-standards` Wenn Sie keinen Standard-ARN angeben, gibt dieser Befehl alle Security Hub-Steuerungs-IDs zurück. Dieser

Befehl gibt standardunabhängige Sicherheitskontroll-IDs zurück, nicht die standardbasierten Kontroll-IDs, die vor diesen Feature-Releases existierten.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Führen Sie den batch-get-security-controls Befehl aus, um Details zu einem oder mehreren Steuerelementen im aktuellen und abzurufen. AWS-Konto AWS-Region

```
aws securityhub --region us-east-1 batch-get-security-controls --security-
control-ids '["Config.1", "IAM.1"]'
```

Die Liste der Steuerelemente filtern und sortieren

Auf der Seite „Steuerelemente“ sehen Sie eine Liste Ihrer Steuerelemente. Sie können die Liste filtern und sortieren, um sich auf eine bestimmte Teilmenge von Steuerelementen zu konzentrieren.

- Alle aktiviert (Steuerelemente, die in mindestens einem aktivierten Standard aktiviert sind)
- Fehlgeschlagen (Steuerelemente mit einem `Failed` Status)
- Unbekannt (Steuerelemente mit einem `Unknown` Status)
- Bestanden (Kontrollen mit einem `Passed` Status)
- Deaktiviert (Steuerelemente, die in allen Standards deaktiviert sind)
- Keine Daten (Kontrollen ohne Ergebnisse)
- Alle (alle Kontrollen, sowohl aktiviert als auch deaktiviert, und unabhängig vom Kontrollstatus oder der Anzahl der Ergebnisse)

Weitere Informationen zum Kontrollstatus finden Sie unterKonformitätsstatus und Kontrollstatus.

Wenn Sie die Integration mit dem AWS Security Hub Administratorkonto verwenden AWS Organizations und dort angemeldet sind, enthält die Registerkarte Alle aktiviert Steuerelemente, die in mindestens einem Mitgliedskonto aktiviert sind. Wenn Sie eine Aggregationsregion festgelegt haben, enthält die Registerkarte „Alle aktiviert“ Steuerelemente, die in mindestens einer verknüpften Region aktiviert sind.

Die Registerkarte Fehlgeschlagen wird standardmäßig angezeigt. Auf jeder Registerkarte sind die Kontrollen standardmäßig nach Schweregrad sortiert, von Kritisch bis Niedrig. Sie können die Kontrollen auch nach Kontroll-ID, Konformitätsstatus, Schweregrad oder Anzahl der fehlgeschlagenen Prüfungen sortieren. In der Suchleiste können Sie nach bestimmten Kontrollen suchen.

> **Tip**
>
> Wenn Sie automatisierte Workflows haben, die auf Kontrollergebnissen basieren, empfehlen wir, die Felder `SecurityControlId` oder `SecurityControlArn` ASFF als Filter zu verwenden und nicht `Title` oder`Description`. Letztere Felder können sich gelegentlich ändern, wohingegen die Kontroll-ID und der ARN statische Identifikatoren sind.

Wenn Sie die Option neben dem Steuerelement auswählen, wird ein Seitenbereich geöffnet, in dem die Standards angezeigt werden, in denen das Steuerelement derzeit aktiviert ist. Sie können auch die Standards sehen, in denen das Steuerelement derzeit deaktiviert ist. In diesem Bereich können Sie ein Steuerelement deaktivieren, indem Sie es in allen Standards deaktivieren. Weitere Informationen zur standardübergreifenden Aktivierung und Deaktivierung von Steuerungen finden Sie unter. Aktivierung und Deaktivierung von Steuerungen in allen Standards Bei Administratorkonten beziehen sich die Informationen im Seitenbereich auf alle Mitgliedskonten.

Führen Sie auf der Security Hub Hub-API `ListSecurityControlDefinitions`den Befehl aus, um eine Liste der Kontroll-IDs abzurufen. Sobald Sie die Kontroll-IDs haben, an denen Sie interessiert sind, führen Sie den Befehl aus, `BatchGetSecurityControls`um Daten zu dieser Teilmenge von Steuerelementen für die aktuelle Version AWS-Konto und AWS-Region abzurufen.

Kontrollergebnisse anzeigen und entsprechende Maßnahmen ergreifen

Auf der Seite mit den Kontrolldetails wird eine Liste der aktiven Ergebnisse für eine Kontrolle angezeigt. Die Liste enthält keine archivierten Ergebnisse.

Die Seite mit den Kontrolldetails unterstützt die Aggregation von Suchbegriffen. Wenn Sie eine Aggregationsregion festgelegt haben, enthalten der Kontrollstatus und die Liste der Sicherheitsüberprüfungen auf der Seite mit den Kontrolldetails die Prüfungen aller verknüpften Kontrollen. AWS-Regionen

Die Liste enthält Tools zum Filtern und Sortieren der Ergebnisse, sodass Sie sich zuerst auf dringendere Ergebnisse konzentrieren können. Ein Ergebnis kann Links zu Ressourcendetails in der

entsprechenden Servicekonsole enthalten. Bei Steuerungen, die auf AWS Config Regeln basieren, können Sie sich Details zur Regel und zum Zeitplan für die Konfiguration anzeigen lassen.

Sie können die AWS Security Hub API auch verwenden, um eine Liste der Ergebnisse abzurufen. Weitere Informationen finden Sie unter the section called “Details zu den Ergebnissen werden überprüft”.

Themen

Details zu einer Kontrollsuche und zu einer Ressource anzeigen

AWS Security Hub enthält die folgenden Details zu jedem Kontrollbefund, um Ihnen bei der Untersuchung zu helfen:

- Eine Historie der Änderungen, die Benutzer an dem Ergebnis vorgenommen haben
- Eine `.json` Datei für den Befund
- Informationen über die Ressource, die sich auf den Befund bezieht
- Die Konfigurationsregel, die sich auf den Befund bezieht
- Hinweise, die Benutzer dem Ergebnis hinzugefügt haben

Im folgenden Abschnitt wird erklärt, wie Sie auf diese Details zugreifen können.

Geschichte finden

Der Suchverlauf ist eine Security Hub Hub-Funktion, mit der Sie Änderungen verfolgen können, die in den letzten 90 Tagen an einem Ergebnis vorgenommen wurden.

Der Suchverlauf ist für Kontrollbefunde und andere Security Hub Hub-Ergebnisse verfügbar. Weitere Informationen finden Sie unter Den Verlauf der Ergebnisse überprüfen.

Anzeige der vollständigen Datei „.json“ für einen Befund

Sie können den vollständigen `.json` Befund anzeigen und herunterladen.

Um das anzuzeigen`.json`, wählen Sie in der Spalte Finding .json das Symbol aus.

Um das herunterzuladen, wählen Sie im Fenster Finding JSON die `.json` Option Herunterladen aus.

Informationen zu einer Suchressource anzeigen

Die Spalte Ressource enthält den Ressourcentyp und die Ressourcen-ID.

Um Informationen über die Ressource anzuzeigen, wählen Sie die Ressourcen-ID. Denn AWS-Konten wenn es sich bei dem Konto um ein Mitgliedskonto einer Organisation handelt, umfassen die Informationen sowohl die Konto-ID als auch den Kontonamen. Bei Konten, die manuell eingeladen wurden, enthalten die Informationen nur die Konto-ID.

Wenn Sie berechtigt sind, die Ressource in ihrem ursprünglichen Dienst anzuzeigen, zeigt die Ressourcen-ID einen Link zu dem Dienst an. Für einen AWS Benutzer stellen die Ressourcendetails beispielsweise einen Link zur Ansicht der Benutzerdetails in IAM bereit.

Wenn sich die Ressource in einem anderen Konto befindet, zeigt Security Hub eine Meldung an, um Sie zu benachrichtigen.

Die Konfigurationszeitleiste für eine gefundene Ressource anzeigen

Eine Möglichkeit der Untersuchung ist der Konfigurationszeitplan für die Ressource in AWS Config.

Wenn Sie berechtigt sind, die Konfigurationszeitleiste für die Suchressource einzusehen, enthält die Ergebnisliste einen Link zur Zeitleiste.

Security Hub zeigt eine Meldung an, um Sie zu benachrichtigen, wenn sich die Ressource in einem anderen Konto befindet.

Um zur Konfigurationszeitleiste zu navigieren in AWS Config

1. Wählen Sie in der Spalte Untersuchen das Symbol aus.
2. Wählen Sie im Menü die Option Konfigurationszeitleiste aus. Wenn Sie keinen Zugriff auf die Konfigurationszeitleiste haben, wird der Link nicht angezeigt.

Die AWS Config Regel für eine Suchressource anzeigen

Wenn das Steuerelement auf einer AWS Config Regel basiert, möchten Sie möglicherweise auch die Details der AWS Config Regel anzeigen. Anhand der AWS Config Regelinformationen können Sie besser verstehen, warum eine Prüfung bestanden wurde oder nicht.

Wenn Sie berechtigt sind, die AWS Config Regel für das Steuerelement einzusehen, enthält die Ergebnisliste einen Link zu der AWS Config Regel unter AWS Config.

Security Hub zeigt eine Meldung an, um Sie zu benachrichtigen, wenn sich die Ressource in einem anderen Konto befindet.

Um zur AWS Config Regel zu navigieren

1. Wählen Sie in der Spalte Untersuchen das Symbol aus.
2. Wählen Sie im Menü Config Rule aus. Wenn Sie keinen Zugriff auf die AWS Config Regel haben, ist die Config-Regel nicht verknüpft.

Hinweise zu Ergebnissen anzeigen

Wenn einem Ergebnis eine Notiz zugeordnet ist, wird in der Spalte Aktualisiert ein Notizsymbol angezeigt.

Um die Notiz anzuzeigen, die mit einem Ergebnis verknüpft ist

Wählen Sie in der Spalte Aktualisiert das Notizsymbol aus.

Ergebnisse der Stichprobenkontrolle

Das Format der Kontrollbefunde hängt davon ab, ob Sie konsolidierte Kontrollbefunde aktiviert haben. Wenn Sie diese Funktion aktivieren, generiert Security Hub einen einzigen Befund für eine Kontrollüberprüfung, auch wenn die Kontrolle für mehrere aktivierte Standards gilt. Weitere Informationen finden Sie unter Konsolidierte Kontrollergebnisse.

Der folgende Abschnitt zeigt Beispiele von Kontrollbefunden. Dazu gehören Ergebnisse aus jedem Security Hub Hub-Standard, wenn konsolidierte Kontrollergebnisse in Ihrem Konto deaktiviert sind, und ein Beispiel für ein standardübergreifendes Kontrollergebnis, wenn es aktiviert ist.

> **Note**
>
> Die Ergebnisse werden sich auf verschiedene Bereiche und Werte in den Regionen und AWS GovCloud (US) Regionen Chinas beziehen. Weitere Informationen finden Sie unter Auswirkungen der Konsolidierung auf ASFF-Felder und -Werte.

Die konsolidierten Kontrollergebnisse sind deaktiviert

- Ergebnis eines Beispiels für den FSBP-Standard (AWS Foundational Security Best Practices)
- Musterbefund für Benchmark v1.2.0 der Center for Internet Security (CIS) AWS Foundations
- Musterbefund für Benchmark v1.4.0 der Center for Internet Security (CIS) AWS Foundations
- Musterbefund für den Benchmark v3.0.0 der Center for Internet Security (CIS) AWS Foundations
- Stichprobenerhebung für SP 800-53 Rev. 5 des National Institute of Standards and Technology (NIST)
- Ergebnis einer Stichprobe für den Datensicherheitsstandard der Zahlungskartenindustrie (PCI DSS)
- Musterbefund für AWS Resource Tagging Standard
- Musterbefund für Service-Managed Standard: AWS Control Tower

Die Option „Konsolidierte Kontrollergebnisse“ ist aktiviert

- Normenübergreifende Stichprobenfindung

Stichprobenfindung für FSBP


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.076Z",
  "LastObservedAt": "2021-09-28T16:10:06.956Z",
  "CreatedAt": "2020-08-06T02:18:23.076Z",
  "UpdatedAt": "2021-09-28T16:10:00.093Z",
  "Severity": {
    "Product": 40,
```

```
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-
practices/v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
```

```
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
    ]
  }
}
```

Beispielbefund für CIS AWS Foundations Benchmark v3.0.0

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
```

```
  "FirstObservedAt": "2024-04-18T07:46:18.193Z",
  "LastObservedAt": "2024-04-23T07:47:01.137Z",
  "CreatedAt": "2024-04-18T07:46:18.193Z",
  "UpdatedAt": "2024-04-23T07:46:46.165Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.2.1 EBS default encryption should be enabled",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
 the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
 at EBS volume creation is supported.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/3.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0",
    "ControlId": "2.2.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2843ed9e",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
```

```
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v3.0.0/2.2.1"
    ],
    "SecurityControlId": "EC2.7",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  },
  "ProcessedAt": "2024-04-23T07:47:07.088Z"
}
```

Musterbefund für CIS AWS Foundations Benchmark v1.4.0

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
```

```
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2022-10-21T22:14:48.913Z",
  "LastObservedAt": "2022-12-22T22:24:56.980Z",
  "CreatedAt": "2022-10-21T22:14:48.913Z",
  "UpdatedAt": "2022-12-22T22:24:52.409Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS CloudTrail is a web service that records AWS API calls for an
 account and makes those logs available to users and resources in accordance with IAM
 policies. AWS Key Management Service (KMS) is a managed service that helps create
 and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs
 can be configured to leverage server side encryption (SSE) and AWS KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
    "ControlId": "3.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
```

```
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
```

```
  }
}
```

Stichprobenergebnis für CIS AWS Foundations Benchmark v1.2.0


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/
rule/2.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2020-08-29T04:10:06.337Z",
  "LastObservedAt": "2021-09-28T16:10:05.350Z",
  "CreatedAt": "2020-08-29T04:10:06.337Z",
  "UpdatedAt": "2021-09-28T16:10:00.087Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS Key Management Service (KMS) is a managed service that helps
 create and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail
 logs can be configured to leverage server side encryption (SSE) and KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
```

```
    }
  },
  "ProductFields": {
    "StandardsGuideArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0",
    "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
    "RuleId": "2.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-
foundations-benchmark/v/1.2.0/2.7",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
```

```
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

Stichprobenfindung für NIST SP 800-53 Rev. 5

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2023-02-17T14:22:46.726Z",
  "LastObservedAt": "2023-02-17T14:22:50.846Z",
  "CreatedAt": "2023-02-17T14:22:46.726Z",
  "UpdatedAt": "2023-02-17T14:22:46.726Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
```

```
      "Text": "For directions on how to fix this issue, consult the AWS Security Hub
 NIST 800-53 R5 documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-53/v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-53/v/5.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/
v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",

      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",

      "Partition": "aws",

      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "NIST.800-53.r5 AU-9",
        "NIST.800-53.r5 CA-9(1)",
        "NIST.800-53.r5 CM-3(6)",
        "NIST.800-53.r5 SC-13",
```

```
        "NIST.800-53.r5 SC-28",
        "NIST.800-53.r5 SC-28(1)",
        "NIST.800-53.r5 SC-7(10)",
        "NIST.800-53.r5 SI-7(6)"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-53/v/5.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2023-02-17T14:22:53.572Z"
}
```

Stichprobenfindung für PCI DSS

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
```

```
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.089Z",
  "LastObservedAt": "2021-09-28T16:10:06.942Z",
  "CreatedAt": "2020-08-06T02:18:23.089Z",
  "UpdatedAt": "2021-09-28T16:10:00.090Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest using AWS KMS
 CMKs",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption by checking if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/pci-dss/v/3.2.1",
    "ControlId": "PCI.CloudTrail.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
```

```
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "PCI DSS 3.4"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/pci-dss/v/3.2.1"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
    ]
  }
}
```

Ein Musterbefund für AWS Resource Tagging Standard

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
```

```
  "Region": "eu-central-1",
  "GeneratorId": "security-control/EC2.44",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-02-19T21:00:32.206Z",
  "LastObservedAt": "2024-04-29T13:01:57.861Z",
  "CreatedAt": "2024-02-19T21:00:32.206Z",
  "UpdatedAt": "2024-04-29T13:01:41.242Z",
  "Severity": {
    "Label": "LOW",
    "Normalized": 1,
    "Original": "LOW"
  },
  "Title": "EC2 subnets should be tagged",
  "Description": "This control checks whether an Amazon EC2 subnet has tags with the
 specific keys defined in the parameter requiredTagKeys. The control fails if the
 subnet doesn't have any tag keys or if it doesn't have all the keys specified in
 the parameter requiredTagKeys. If the parameter requiredTagKeys isn't provided, the
 control only checks for the existence of a tag key and fails if the subnet isn't
 tagged with any key. System tags, which are automatically applied and begin with aws:,
 are ignored.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.44/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-tagged-ec2-subnet-6ceafede",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "No tags are present.",
    "Resources:0/Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
securityhub/arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
```

```
      "Type": "AwsEc2Subnet",
      "Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/subnet-1234567890abcdef0",
      "Partition": "aws",
      "Region": "eu-central-1",
      "Details": {
        "AwsEc2Subnet": {
          "AssignIpv6AddressOnCreation": false,
          "AvailabilityZone": "eu-central-1b",
          "AvailabilityZoneId": "euc1-az3",
          "AvailableIpAddressCount": 4091,
          "CidrBlock": "10.24.34.0/23",
          "DefaultForAz": true,
          "MapPublicIpOnLaunch": true,
          "OwnerId": "123456789012",
          "State": "available",
          "SubnetArn": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
          "SubnetId": "subnet-1234567890abcdef0",
          "VpcId": "vpc-021345abcdef6789"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.44",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/aws-resource-tagging-standard/v/1.0.0"
      }
    ],
    "SecurityControlParameters": [
      {
        "Name": "requiredTagKeys",
        "Value": [
          "peepoo"
        ]
      }
    ],
            },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
```

```
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "LOW",
      "Original": "LOW"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2024-04-29T13:02:03.259Z"
}
```

Musterbefund für Service-Managed Standard: AWS Control Tower

> **Note**
>
> Dieser Standard steht Ihnen nur zur Verfügung, wenn Sie ein AWS Control Tower Benutzer sind, der den Standard in AWS Control Tower erstellt hat. Weitere Informationen finden Sie unter Vom Service verwalteter Standard: AWS Control Tower.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-
control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-11-17T01:25:30.296Z",
  "LastObservedAt": "2022-11-17T01:25:45.805Z",
  "CreatedAt": "2022-11-17T01:25:30.296Z",
  "UpdatedAt": "2022-11-17T01:25:30.296Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
```

```
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/service-managed-aws-control-tower/
v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
    "ControlId": "CT.CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-
managed-aws-control-tower/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-
aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
```

```
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}
```

Standardübergreifende Stichprobenermittlung (wenn die Option „Konsolidierte Kontrollergebnisse“ aktiviert ist)

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "security-control/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-10-06T02:18:23.076Z",
  "LastObservedAt": "2022-10-28T16:10:06.956Z",
  "CreatedAt": "2022-10-06T02:18:23.076Z",
  "UpdatedAt": "2022-10-28T16:10:00.093Z",
  "Severity": {
```

```
    "Label": "MEDIUM",
    "Normalized": "40",
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  }
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "PCI DSS v3.2.1/3.4",
        "CIS AWS Foundations Benchmark v1.2.0/2.7",
        "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
```

```
    "AssociatedStandards": [
       { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
       { "StandardsId": "standards/pci-dss/v/3.2.1"},
       { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
       { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
       { "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}
```

Filtern, Sortieren und Herunterladen von Kontrollbefunden

Sie können die Liste der Kontrollergebnisse anhand des Konformitätsstatus filtern, indem Sie die Filterregisterkarten verwenden. Sie können die Liste auch anhand anderer Ergebnisfeldwerte filtern und Ergebnisse aus der Liste herunterladen.

Filtern und Sortieren der Kontroll-Suchliste

Auf der Registerkarte Alle Prüfungen werden alle aktiven Ergebnisse aufgeführt, die den Workflow-Status `NEW``NOTIFIED`, oder haben`RESOLVED`. Standardmäßig ist die Liste so sortiert, dass fehlgeschlagene Ergebnisse ganz oben in der Liste stehen. Diese Sortierreihenfolge hilft Ihnen dabei, Ergebnisse zu priorisieren, die behoben werden müssen.

Die Listen auf den Registerkarten Fehlgeschlagen, Unbekannt und Bestanden werden nach dem Wert von `Compliance.Status` gefiltert. Die Listen enthalten auch nur aktive Ergebnisse, die den Workflow-Status `NEW``NOTIFIED`, oder haben`RESOLVED`.

Die Registerkarte Unterdrückt enthält eine Liste der aktiven Ergebnisse mit dem Workflow-Status. `SUPPRESSED`

Zusätzlich zu den integrierten Filtern auf jeder Registerkarte können Sie die Listen anhand von Werten aus den folgenden Feldern filtern:

- Konto-ID
- Workflow-Status
- Compliance status (Compliance-Status)
- Ressourcen-ID
- Ressourcentyp

Sie können jede Liste anhand einer beliebigen Spalte sortieren.

Die Liste der Kontrollergebnisse wird heruntergeladen

Wenn Sie zu Sicherheitsstandards navigieren und einen Standard auswählen, wird eine Liste der Kontrollen für diesen Standard angezeigt. Wenn Sie ein Steuerelement aus der Liste auswählen, gelangen Sie zur Seite mit den Kontrolldetails mit einer Liste der Ergebnisse für das Steuerelement. Von hier aus können Sie die Kontrollergebnisse in eine CSV-Datei herunterladen.

Wenn Sie die Ergebnisliste filtern, umfasst der Download nur die Steuerelemente, die dem Filter entsprechen.

Wenn Sie bestimmte Ergebnisse aus der Liste auswählen, enthält der Download nur die ausgewählten Ergebnisse.

Um die Ergebnisse herunterzuladen, wählen Sie Herunterladen. Die aktuelle Seite mit den Ergebnissen wird heruntergeladen.

Ergreifen von Maßnahmen auf der Grundlage der Kontrollergebnisse

Um den aktuellen Status Ihrer Untersuchung widerzuspiegeln, legen Sie den Workflow-Status fest. Weitere Informationen finden Sie unter the section called “Den Workflow-Status von Ergebnissen festlegen”.

AWS Security Hub In können Sie auch ausgewählte Ergebnisse an eine benutzerdefinierte Aktion in Amazon senden EventBridge. Weitere Informationen finden Sie unter the section called “Senden von Ergebnissen an eine benutzerdefinierte Aktion”.

Mit dem Übersichts-Dashboard arbeiten

In der AWS Security Hub Hub-Konsole kann Ihnen das Dashboard auf der Übersichtsseite dabei helfen, Bereiche zu identifizieren, in denen Sicherheitsbedenken in Ihrer AWS Umgebung bestehen, ohne dass zusätzliche Analysetools oder komplexe Abfragen erforderlich sind. Sie können das Dashboard-Layout anpassen, Widgets hinzufügen oder entfernen und die Daten filtern, um sich auf Bereiche von besonderem Interesse zu konzentrieren. Sie können Ihre Filterkriterien auch als Filtersatz speichern, um in future schnell bestimmte Datentypen abzurufen.

Wenn Sie das Dashboard anpassen oder die Daten filtern, speichert Security Hub Ihre Einstellungen automatisch für die spätere Verwendung. Darüber hinaus werden die Einstellungen für jeden Benutzer Ihres Security Hub Hub-Kontos unabhängig gespeichert. Das bedeutet, dass verschiedene Benutzer unterschiedliche Layouts, Widgets und Filtersätze für das Dashboard haben können.

Jedes Mal, wenn Sie das Übersichts-Dashboard öffnen, aktualisiert Security Hub automatisch die meisten Dashboard-Daten. Einige Daten werden jedoch seltener aktualisiert. Beispielsweise werden Sicherheitswerte und Kontrollstatus alle 24 Stunden aktualisiert.

Wenn Sie eine regionsübergreifende Aggregationsregion für Security Hub konfiguriert haben, enthalten Ihre Dashboard-Daten Ergebnisse aus der Aggregationsregion und allen verknüpften Regionen. Wenn Sie der delegierte Security Hub-Administrator für eine Organisation sind, umfassen die Daten Ergebnisse für Ihr Administratorkonto und Ihre Mitgliedskonten. Sie können die Daten optional nach Konto filtern. Wenn Sie ein Mitgliedskonto oder ein eigenständiges Konto haben, enthalten die Daten nur Ergebnisse für Ihr Konto.

Verfügbare Widgets für das Übersichts-Dashboard

Das Übersichts-Dashboard enthält Widgets, die die aktuelle Bedrohungslandschaft der Cloud-Sicherheit widerspiegeln und sich dabei an den Sicherheitsabläufen und Erfahrungen der AWS Kunden orientieren. Einige Widgets werden standardmäßig angezeigt, andere nicht. Sie können Ihre Ansicht des Dashboards anpassen, indem Sie Widgets hinzufügen oder entfernen.

Um sie hinzuzufügen, wählen Sie oben rechts auf der Übersichtsseite Widget hinzufügen. Geben Sie in der Suchleiste den Titel des Widgets ein. Ziehen Sie das Widget per Drag & Drop auf das Dashboard.

Standardmäßig werden Widgets angezeigt

Standardmäßig enthält das Übersichts-Dashboard die folgenden Widgets:

Sicherheitsstandards

Zeigt Ihre aktuelle zusammenfassende Sicherheitsbewertung und die Sicherheitsbewertung für jeden Security Hub Hub-Standard an. Sicherheitswerte, die zwischen 0 und 100 Prozent liegen, stellen den Anteil der bestandenen Kontrollen im Verhältnis zu allen aktivierten Kontrollen dar. Weitere Informationen zu diesen Bewertungen finden Sie unter. Wie werden Sicherheitswerte berechnet Dieses Widget hilft Ihnen dabei, Ihren allgemeinen Sicherheitsstatus zu verstehen.

Anlagen mit den meisten Ergebnissen

Bietet einen Überblick über die Ressourcen, Konten und Anwendungen mit den meisten Ergebnissen. Die Liste ist in absteigender Reihenfolge nach der Anzahl der Ergebnisse sortiert. Im Widget zeigt jede Registerkarte die sechs wichtigsten Elemente in dieser Kategorie, gruppiert nach Schweregrad und Ressourcentyp. Wenn Sie in der Spalte Ergebnisse insgesamt eine Zahl auswählen, öffnet Security Hub eine Seite, auf der die Ergebnisse für das Asset angezeigt werden. Mit diesem Widget können Sie schnell erkennen, welche Ihrer Kernressourcen potenzielle Sicherheitsbedrohungen bergen.

Ergebnisse nach Regionen

Zeigt die Gesamtzahl der Ergebnisse, gruppiert nach Schweregrad, in jedem Fall an, AWS-Region in dem Security Hub aktiviert ist. Dieses Widget hilft Ihnen dabei, Sicherheitsprobleme zu identifizieren, die möglicherweise bestimmte Regionen betreffen. Wenn Sie das Dashboard in Ihrer Aggregationsregion öffnen, hilft Ihnen dieses Widget dabei, potenzielle Sicherheitsprobleme in jeder verknüpften Region zu überwachen.

Die häufigsten Bedrohungsarten

Bietet eine Aufschlüsselung der 10 häufigsten Bedrohungstypen in Ihrer AWS Umgebung. Dazu gehören Bedrohungen wie die Eskalation von Rechten, die Verwendung offengelegter Anmeldeinformationen oder die Kommunikation mit bösartigen IP-Adressen.

Um diese Daten anzeigen zu können, GuardDuty muss Amazon aktiviert sein. Wenn ja, wählen Sie in diesem Widget einen Bedrohungstyp aus, um die GuardDuty Konsole zu öffnen und die Ergebnisse zu dieser Bedrohung zu überprüfen. Dieses Widget hilft Ihnen dabei, potenzielle Bedrohungen im Zusammenhang mit anderen Sicherheitsproblemen zu bewerten.

Sicherheitslücken in Software durch Exploits

Bietet eine Zusammenfassung der Softwareschwachstellen, die in Ihrer AWS Umgebung vorhanden sind und für die bekannte Exploits bekannt sind. Sie können sich auch eine Aufschlüsselung der Sicherheitslücken ansehen, für die es Lösungen gibt und für die es keine gibt.

Um diese Daten anzeigen zu können, muss Amazon Inspector aktiviert sein. Wenn ja, wählen Sie eine Statistik in diesem Widget aus, um die Amazon Inspector Inspector-Konsole zu öffnen und weitere Details zu der Sicherheitslücke zu überprüfen. Dieses Widget hilft Ihnen dabei, Softwareschwachstellen im Zusammenhang mit anderen Sicherheitsproblemen zu bewerten.

Neue Erkenntnisse im Laufe der Zeit

Zeigt Trends bei der Anzahl neuer täglicher Ergebnisse in den letzten 90 Tagen. Sie können die Daten nach Schweregrad oder nach Anbieter aufschlüsseln, um zusätzlichen Kontext zu erhalten. Mithilfe dieses Widgets können Sie nachvollziehen, ob das gefundene Volumen in den letzten 90 Tagen zu bestimmten Zeiten angestiegen oder gesunken ist.

Ressourcen mit den meisten Ergebnissen

Bietet eine Zusammenfassung der Ressourcen, die zu den meisten Ergebnissen geführt haben, aufgeschlüsselt nach den folgenden Ressourcentypen: Amazon Simple Storage Service (Amazon S3) -Buckets, Amazon Elastic Compute Cloud (Amazon EC2) -Instances und AWS Lambda Funktionen.

Im Widget konzentriert sich jede Registerkarte auf einen der vorherigen Ressourcentypen und listet die 10 Ressourcen-Instances auf, die die meisten Ergebnisse generiert haben. Um die Ergebnisse für eine bestimmte Ressource zu überprüfen, wählen Sie die Ressourceninstanz aus. Dieses Widget hilft Ihnen bei der Suche nach Sicherheitsergebnissen, die mit gängigen AWS Ressourcen verknüpft sind.

Widgets sind standardmäßig ausgeblendet

Die folgenden Widgets sind auch für das Übersichts-Dashboard verfügbar, sie sind jedoch standardmäßig ausgeblendet:

AMIs mit den meisten Ergebnissen

Stellt eine Liste der 10 Amazon Machine Images (AMIs) bereit, die die meisten Ergebnisse generiert haben. Diese Daten sind nur verfügbar, wenn Amazon EC2 für Ihr Konto aktiviert ist. Auf diese Weise können Sie ermitteln, welche AMIs potenzielle Sicherheitsrisiken darstellen.

IAM-Prinzipale mit den meisten Ergebnissen

Stellt eine Liste der 10 AWS Identity and Access Management (IAM) -Benutzer bereit, die die meisten Ergebnisse generiert haben. Dieses Widget hilft Ihnen bei der Ausführung von Verwaltungs- und Abrechnungsaufgaben. Es zeigt Ihnen, welche Benutzer am meisten zur Nutzung von Security Hub beitragen.

Konten mit den meisten Ergebnissen (nach Schweregrad)

Zeigt eine grafische Darstellung der 10 Konten, die die meisten Ergebnisse generiert haben, gruppiert nach Schweregrad. Mithilfe dieses Widgets können Sie bestimmen, auf welche Konten Sie sich bei der Analyse und Problembehebung konzentrieren sollten.

Konten mit den meisten Ergebnissen (nach Ressourcentyp)

Zeigt ein Diagramm der 10 Konten, die die meisten Ergebnisse generiert haben, gruppiert nach Ressourcentyp. Mit diesem Widget können Sie bestimmen, welche Konten und Ressourcentypen für die Analyse und Problembehebung priorisiert werden müssen.

Einblicke

Führt fünf von Security Hub verwaltete Erkenntnisse und die Anzahl der Ergebnisse auf, die sie generiert haben. Insights identifizieren einen bestimmten Sicherheitsbereich, der Aufmerksamkeit erfordert.

Aktuelle Erkenntnisse aus AWS Integrationen

Zeigt die Anzahl der Ergebnisse an, die Sie in Security Hub von integrated erhalten habenAWS-Services. Außerdem wird angezeigt, wann Sie zuletzt Ergebnisse von den einzelnen integrierten Diensten erhalten haben. Dieses Widget bietet konsolidierte Ergebnisdaten aus mehrerenAWS-Services. Wählen Sie einen integrierten Service aus, um weitere Informationen zu erhalten. Security Hub öffnet dann die Konsole für diesen Dienst.

Das Übersichts-Dashboard filtern

Um die Daten im Übersichts-Dashboard zu kuratieren und nur die Sicherheitsdaten einzubeziehen, die für Sie am relevantesten sind, können Sie das Dashboard filtern. Wenn Sie beispielsweise

Mitglied eines Anwendungsteams sind, können Sie eine spezielle Ansicht für eine wichtige Anwendung in Ihrer Produktionsumgebung erstellen. Wenn Sie Mitglied eines Sicherheitsteams sind, können Sie eine spezielle Ansicht erstellen, die Ihnen hilft, sich auf Ergebnisse mit hohem Schweregrad zu konzentrieren. Um Daten im Übersichts-Dashboard zu filtern, geben Sie Filterkriterien in das Filterfeld über dem Dashboard ein. Wenn Sie Filterkriterien anwenden, gelten die Kriterien für alle Daten im Dashboard mit Ausnahme der Daten in den Widgets „Einblicke“ und „Sicherheitsstandards“.

Sie können die Daten mithilfe der folgenden Felder filtern:

- Account name (Kontoname)
- Konto-ID
- Amazon-Ressourcenname (ARN) der Anwendung
- Anwendungsname
- Produktname (für ein Produkt AWS-Service oder ein Produkt eines Drittanbieters, das Ergebnisse an Security Hub sendet)
- Record state (Datensatzstatus)
- Region
- Ressourcen-Tag
- Schweregrad
- Workflow-Status

Standardmäßig werden Dashboard-Daten anhand der folgenden Kriterien gefiltert: `Workflow status` ist `NOTIFIED` oder`NEW`, und `Record state` ist`ACTIVE`. Diese Kriterien werden über dem Dashboard unter dem Filterfeld angezeigt. Um diese Kriterien zu entfernen, wählen Sie X im Filtertoken für die Kriterien, die Sie entfernen möchten.

Wenn Sie Filterkriterien anwenden, die Sie erneut verwenden möchten, können Sie sie als Filtersatz speichern. Ein Filtersatz besteht aus einer Reihe von Filterkriterien, die Sie erstellen und speichern, um sie erneut anzuwenden, wenn Sie Daten im Übersichts-Dashboard überprüfen.

> **Note**
>
> Die folgenden Felder können nicht als Teil eines Filtersatzes gespeichert werden: Anwendungs-ARN, Anwendungsname und Ressourcen-Tag.

Filtersätze erstellen und speichern

Gehen Sie wie folgt vor, um einen Filtersatz zu erstellen und zu speichern.

Um einen Filtersatz zu erstellen und zu speichern

1. Öffnen Sie die AWS Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Zusammenfassung aus.
3. Geben Sie im Filterfeld über dem Übersichts-Dashboard die Filterkriterien für den Filtersatz ein.
4. Wählen Sie im Menü Filter löschen die Option Neuen Filtersatz speichern aus.
5. Geben Sie im Dialogfeld Filtersatz speichern einen Namen für den Filtersatz ein.
6. (Optional) Um den Filtersatz bei jedem Öffnen der Übersichtsseite standardmäßig zu verwenden, wählen Sie die Option, um ihn als Standardansicht festzulegen.
7. Wählen Sie Speichern aus.

Um zwischen den von Ihnen erstellten und gespeicherten Filtersätzen zu wechseln, verwenden Sie das Menü „Filtersatz auswählen“ über dem Übersichts-Dashboard. Wenn Sie einen Filtersatz auswählen, wendet Security Hub die Kriterien des Filtersatzes auf die Daten im Dashboard an.

Filtersätze aktualisieren oder löschen

Gehen Sie wie folgt vor, um einen vorhandenen Filtersatz zu aktualisieren oder zu löschen. Wenn Sie einen Filtersatz löschen, der derzeit als Standardansicht des Übersichts-Dashboards eingerichtet ist, wird Ihre Standardansicht auf die Security Hub Hub-Standardansicht zurückgesetzt.

Um einen Filtersatz zu aktualisieren oder zu löschen

1. Öffnen Sie die AWS Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Zusammenfassung aus.
3. Wählen Sie im Menü Wählen Sie einen Filtersatz über der Übersichtsseite den Filtersatz aus.
4. Führen Sie im Menü Filter löschen einen der folgenden Schritte aus:
   - Um den Filtersatz zu aktualisieren, wählen Sie Aktuellen Filtersatz aktualisieren. Geben Sie dann Ihre Änderungen in das angezeigte Dialogfeld ein.

- Um den Filtersatz zu löschen, wählen Sie Aktuellen Filtersatz löschen. Wählen Sie anschließend im daraufhin angezeigten Dialogfeld die Option Löschen.

Anpassen des Übersichts-Dashboards

Sie können das Übersichts-Dashboard auf verschiedene Arten anpassen. Sie können dem Dashboard Widgets hinzufügen und daraus entfernen. Sie können Widgets im Dashboard auch neu anordnen und ihre Größe ändern.

Wenn Sie das Dashboard anpassen, wendet Security Hub Ihre Änderungen sofort an und speichert Ihre neuen Dashboard-Einstellungen. Ihre Änderungen gelten für Ihre Ansicht des Dashboards in allen AWS-Regionen Browsern.

So passen Sie das Übersichts-Dashboard an

1. Öffnen Sie die AWS Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Zusammenfassung aus.
3. Führen Sie eine der folgenden Aktionen aus:

   - Um ein Widget hinzuzufügen, wählen Sie in der oberen rechten Ecke der Seite Widgets hinzufügen. Geben Sie in der Suchleiste den Titel des Widgets ein, das Sie hinzufügen möchten. Ziehen Sie dann das Widget an die gewünschte Position.
   - Um ein Widget zu entfernen, wählen Sie die drei Punkte in der oberen rechten Ecke des Widgets aus.
   - Um ein Widget zu verschieben, wählen Sie den Ziehpunkt in der oberen linken Ecke des Widgets aus und ziehen Sie das Widget dann an die gewünschte Position.
   - Um die Größe eines Widgets zu ändern, wählen Sie den Ziehpunkt zur Größenänderung in der unteren rechten Ecke des Widgets. Ziehen Sie den Rand des Widgets, bis das Widget Ihre bevorzugte Größe hat.

Um anschließend die ursprünglichen Einstellungen wiederherzustellen, wählen Sie „Auf Standardlayout zurücksetzen“ oben auf der Seite.

Security Hub Hub-Ressourcen erstellen mit AWS CloudFormation

AWS Security Hub integriert in. AWS CloudFormation Dabei handelt es sich um einen Service, der Sie bei der Modellierung und Einrichtung Ihrer AWS Ressourcen unterstützt, sodass Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen müssen. Sie erstellen eine Vorlage, die alle gewünschten AWS Ressourcen beschreibt (z. B. Automatisierungsregeln) und diese Ressourcen für Sie AWS CloudFormation bereitstellt und konfiguriert.

Wenn Sie es verwenden AWS CloudFormation, können Sie Ihre Vorlage wiederverwenden, um Ihre Security Hub Hub-Ressourcen konsistent und wiederholt einzurichten. Beschreiben Sie Ihre Ressourcen einmal und stellen Sie dann dieselben Ressourcen immer wieder in mehreren AWS-Konten Regionen bereit.

Security Hub und AWS CloudFormation Vorlagen

Um Ressourcen für Security Hub und verwandte Dienste bereitzustellen und zu konfigurieren, müssen Sie wissen, wie AWS CloudFormation Vorlagen funktionieren. Vorlagen sind Textdateien im JSON- oder YAML-Format. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS CloudFormation Stacks bereitstellen möchten.

Wenn Sie mit JSON oder YAML nicht vertraut sind, können Sie AWS CloudFormation Designer verwenden, um Ihnen die ersten Schritte mit Vorlagen zu erleichtern. AWS CloudFormation Weitere Informationen finden Sie unter Was ist AWS CloudFormation Designer? im AWS CloudFormation Benutzerhandbuch.

Sie können AWS CloudFormation Vorlagen für die folgenden Typen von Security Hub Hub-Ressourcen erstellen:

- Security Hub aktivieren
- Den delegierten Security Hub-Administrator für eine Organisation benennen
- Aktivierung eines Sicherheitsstandards
- Einen benutzerdefinierten Einblick erstellen
- Eine Automatisierungsregel erstellen
- Abonnieren Sie eine Produktintegration eines Drittanbieters

Weitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für Ressourcen, finden Sie in der Referenz zum AWS Security Hub Ressourcentyp im AWS CloudFormation Benutzerhandbuch.

Erfahren Sie mehr über AWS CloudFormation

Weitere Informationen AWS CloudFormation finden Sie in den folgenden Ressourcen:

- AWS CloudFormation
- AWS CloudFormation Benutzerhandbuch
- AWS CloudFormation API Reference
- AWS CloudFormation Benutzerhandbuch für die Befehlszeilenschnittstelle

Security Hub Hub-Ankündigungen mit Amazon Simple Notification Service abonnieren

Dieser Abschnitt enthält Informationen zum Abonnieren von AWS Security Hub-Ankündigungen mit Amazon Simple Notification Service (Amazon SNS), um Benachrichtigungen über Security Hub zu erhalten.

Nach dem Abonnieren erhalten Sie Benachrichtigungen über die folgenden Ereignisse (beachten Sie die entsprechenden Informationen `AnnouncementType` für jedes Ereignis):

- `GENERAL`— Allgemeine Benachrichtigungen über den Security Hub Hub-Dienst.
- `UPCOMING_STANDARDS_CONTROLS`— Spezifizierte Security Hub-Steuerelemente oder -Standards werden in Kürze veröffentlicht. Diese Art der Ankündigung hilft Ihnen dabei, Reaktions- und Behebungsabläufe im Vorfeld einer Veröffentlichung vorzubereiten.
- `NEW_REGIONS`— Die Support für Security Hub ist in einer neuen Version verfügbarAWS-Region.
- `NEW_STANDARDS_CONTROLS`— Neue Security Hub-Steuerelemente oder -Standards wurden hinzugefügt.
- `UPDATED_STANDARDS_CONTROLS`— Bestehende Security Hub-Steuerungen oder -Standards wurden aktualisiert.
- `RETIRED_STANDARDS_CONTROLS`— Bestehende Security Hub Hub-Kontrollen oder -Standards wurden eingestellt.
- `UPDATED_ASFF`— Die Syntax, Felder oder Werte des AWS Security Finding Format (ASFF) wurden aktualisiert.
- `NEW_INTEGRATION`— Neue Integrationen mit anderen AWS Diensten oder Produkten von Drittanbietern sind verfügbar.
- `NEW_FEATURE`— Neue Security Hub Hub-Funktionen sind verfügbar.
- `UPDATED_FEATURE`— Bestehende Security Hub Hub-Funktionen wurden aktualisiert.

Benachrichtigungen sind in allen Formaten verfügbar, die Amazon SNS unterstützt. Sie können Security Hub-Ankündigungen in allen Bereichen abonnieren AWS-Regionen, in denen Security Hub verfügbar ist.

Ein Benutzer muss über `Subscribe` Berechtigungen verfügen, um ein Amazon SNS SNS-Thema zu abonnieren. Sie können dies mit Amazon SNS SNS-Richtlinien, IAM-Richtlinien oder beidem

erreichen. Weitere Informationen finden Sie unter IAM- und Amazon SNS SNS-Richtlinien zusammen im Amazon Simple Notification Service Developer Guide.

> **Note**
>
> Security Hub sendet Amazon SNS SNS-Ankündigungen über Updates für den Security Hub-Service an alle AbonnentenAWS-Konto. Informationen zum Erhalt von Benachrichtigungen über Ergebnisse von Security Hub finden Sie unterVerwaltung und Überprüfung der Funddetails und des Verlaufs.

Sie können eine Amazon Simple Queue Service (Amazon SQS) -Warteschlange für ein Amazon SNS SNS-Thema abonnieren, müssen jedoch einen Amazon SNS SNS-Thema Amazon Resource Name (ARN) verwenden, der sich in derselben Region befindet. Weitere Informationen finden Sie unter Tutorial: Abonnieren einer Amazon SQS SQS-Warteschlange für ein Amazon SNS SNS-Thema im Amazon Simple Queue Service Developer Guide.

Sie können auch eine AWS Lambda Funktion verwenden, um Ereignisse auszulösen, wenn Sie Benachrichtigungen erhalten. Weitere Informationen, einschließlich Beispielfunktionscode, finden Sie unter Tutorial: Using AWS Lambda with Amazon Simple Notification Service im AWS LambdaEntwicklerhandbuch.

Die Amazon SNS SNS-Themen-ARNs für jede Region lauten wie folgt.

AWS-Region	ARN des Amazon-SNS-Themas
US East (Ohio)	`arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements`
USA Ost (Nord-Virginia)	`arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements`
USA West (Nordkalifornien)	`arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements`

AWS-Region	ARN des Amazon-SNS-Themas
USA West (Oregon)	`arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`
Africa (Cape Town)	`arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements`
Asien-Pazifik (Hongkong)	`arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements`
Asien-Pazifik (Hyderabad)	`arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements`
Asien-Pazifik (Jakarta)	`arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements`
Asien-Pazifik (Mumbai)	`arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements`
Asia Pacific (Osaka)	`arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements`
Asia Pacific (Seoul)	`arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements`
Asien-Pazifik (Singapur)	`arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements`

AWS-Region	ARN des Amazon-SNS-Themas
Asien-Pazifik (Sydney)	`arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements`
Asien-Pazifik (Tokio)	`arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements`
Canada (Central)	`arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements`
China (Peking)	`arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements`
China (Ningxia)	`arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements`
Europe (Frankfurt)	`arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements`
Europa (Irland)	`arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements`
Europa (London)	`arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements`
Europa (Milan)	`arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements`

AWS-Region	ARN des Amazon-SNS-Themas
Europa (Paris)	`arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements`
Europa (Spain)	`arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements`
Europa (Stockholm)	`arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements`
Europa (Zürich)	`arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements`
Israel (Tel Aviv)	`arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements`
Naher Osten (Bahrain)	`arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements`
Naher Osten (VAE)	`arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements`
Südamerika (São Paulo)	`arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements`
AWS GovCloud (US-Ost)	`arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements`

AWS-Region	ARN des Amazon-SNS-Themas
AWS GovCloud (US-West)	`arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements`

Nachrichten sind in der Regel in allen Regionen innerhalb einer Partition identisch. Sie können also eine Region in jeder Partition abonnieren, um Ankündigungen zu erhalten, die sich auf alle Regionen in dieser Partition auswirken. Ankündigungen, die mit Mitgliedskonten verknüpft sind, werden nicht im Administratorkonto repliziert. Daher verfügt jedes Konto, einschließlich des Administratorkontos, nur über eine Kopie jeder Ankündigung. Sie können entscheiden, welches Konto Sie verwenden möchten, um Security Hub Hub-Ankündigungen zu abonnieren.

Informationen zu den Kosten für das Abonnieren von Security Hub Hub-Ankündigungen finden Sie unter Amazon SNS SNS-Preise.

Security Hub Hub-Ankündigungen abonnieren (Konsole)

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie in der Liste Region die Region aus, in der Sie Security Hub Hub-Ankündigungen abonnieren möchten. In diesem Beispiel wird die Region `us-west-2` verwendet.
3. Wählen Sie im Navigationsbereich Subscriptions (Abonnements) und dann Create subscription (Abonnement erstellen) aus.
4. Geben Sie den Themen-ARN in das Feld Themen-ARN ein. Zum Beispiel `arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`.
5. Wählen Sie unter Protokoll aus, wie Sie Security Hub Hub-Ankündigungen erhalten möchten. Wenn Sie E-Mail wählen, geben Sie für Endpoint die E-Mail-Adresse ein, die Sie für den Empfang von Ankündigungen verwenden möchten.
6. Wählen Sie Create subscription (Abonnement erstellen) aus.
7. Bestätigen Sie das Abonnement. Wenn Sie beispielsweise das E-Mail-Protokoll ausgewählt haben, sendet Amazon SNS eine Bestätigungsnachricht für das Abonnement an die von Ihnen angegebene E-Mail-Adresse.

Security Hub Hub-Ankündigungen abonnieren () AWS CLI

1. Führen Sie den folgenden Befehl aus:

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. Bestätigen Sie das Abonnement. Wenn Sie beispielsweise das E-Mail-Protokoll ausgewählt haben, sendet Amazon SNS eine Bestätigungsnachricht für das Abonnement an die von Ihnen angegebene E-Mail-Adresse.

Amazon-SNS-Nachrichtenformat

Die folgenden Beispiele zeigen Security Hub Hub-Ankündigungen von Amazon SNS zur Einführung neuer Sicherheitskontrollen. Der Nachrichteninhalt variiert je nach Art der Ankündigung, aber das Format ist für alle Ankündigungstypen gleich. Optional kann ein `Link` Feld mit Details zur Ankündigung hinzugefügt werden.

Beispiel: Security Hub Hub-Ankündigung für neue Kontrollen (E-Mail-Protokoll)

```
{
"AnnouncementType":"NEW_STANDARDS_CONTROLS",
"Title":"[New Controls] 36 new Security Hub controls added to the AWS Foundational
 Security Best Practices standard",
"Description":"We have added 36 new controls to the AWS Foundational Security Best
 Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3,
 AutoScaling.4, AutoScaling.6), AWS CloudFormation (CloudFormation.1), Amazon
 CloudFront (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23,
 EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon
 Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12),
 Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes
 Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon
 Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3, NetworkFirewall.4,
 NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift
 (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
 (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
 Foundational Security Best Practices standard in an account and configured Security
 Hub to automatically enable new controls, these controls are enabled by default.
 Availability of controls can vary by Region. "
}
```

Beispiel: Security Hub Hub-Ankündigung für neue Kontrollen (E-Mail-JSON-Protokoll)

```
{
  "Type" : "Notification",
  "MessageId" : "d124c9cf-326a-5931-9263-92a92e7af49f",
  "TopicArn" : "arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements",
  "Message" : "{\"AnnouncementType\":\"NEW_STANDARDS_CONTROLS\",\"Title\":\"[New
 Controls] 36 new Security Hub controls added to the AWS Foundational Security Best
 Practices standard\",\"Description\":\"We have added 36 new controls to the AWS
 Foundational Security Best Practices standard. These include controls for Amazon
 Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), AWS CloudFormation
 (CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud
 (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR)
 (ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5,
 ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon
 Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12,
 ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3,
 NetworkFirewall.4, NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7),
 Amazon Redshift (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
 (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
 Foundational Security Best Practices standard in an account and configured SSecurity
 Hub to automatically enable new controls, these controls are enabled by default.
 Availability of controls can vary by Region. \"}",
  "Timestamp" : "2022-08-04T19:11:12.652Z",
  "SignatureVersion" : "1",
  "Signature" :
 "HTHgNFRYMetCvisulgLM4CVySvK9qCXFPHQDxYl9tuCFQuIrd7YO4m4YFR28XKMgzqrF20YP
+EilipUm2SOTpEEtOTekU5bn74+YmNZfwr4aPFx0vUuQCVOshmHl37hjkiLjhCg/t53QQiLfP7MH
+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUsOG8yiJVCBEJhJ1yS
+gkwJdhRk2UQab9RcAmE6COK3hRWcjDwqTXz5nR6Ywv1ZqZfLIl7gYKslt+jsyd/k+7kOqGmOJRDr7qhE7H
+7vaGRLOptsQnbW8VmeYnDbahEO8FV+Mp1rpV+7Qg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}
```

Sicherheit in AWS Security Hub

Die Sicherheit in der Cloud hat für AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit gilt zwischen AWS und Ihnen eine geteilte Verantwortung. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud: AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS-Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen für AWS Security Hub finden Sie unter Durch das Compliance-Programm abgedeckte AWS-Services.
- Sicherheit in der Cloud: Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der geteilten Verantwortung bei der Verwendung von Security Hub einsetzen können. Die folgenden Themen zeigen Ihnen, wie Sie Security Hub konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere -AWSServices verwenden, die Sie bei der Überwachung und Sicherung Ihrer Security Hub-Ressourcen unterstützen.

Themen

Datenschutz in AWS Security Hub

Das Modell der geteilten Verantwortung von AWS gilt für den Datenschutz in AWS Security Hub. Wie in diesem Modell beschrieben, ist AWS verantwortlich für den Schutz der globalen Infrastruktur, in der die gesamte AWS Cloud ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS-Modell der geteilten Verantwortung und in der DSGVO im AWS-Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, AWS-Konto-Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Security Hub oder anderen AWS-Services über die KonsoleAWS CLI, API oder AWS SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Security Hub ist ein Serviceangebot für mehrere Mandanten. Um den Datenschutz zu gewährleisten, verschlüsselt Security Hub ruhende Daten und Daten, die zwischen Komponentendiensten übertragen werden.

AWS Identity and Access Management für AWS Security Hub

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Security Hub Hub-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Security Hub ausführen.

Dienstbenutzer — Wenn Sie den Security Hub Hub-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Da Sie für Ihre Arbeit mehr Security Hub Hub-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie auf eine Funktion in Security Hub nicht zugreifen können, finden Sie weitere Informationen unterFehlerbehebung für AWS Security Hub-Identität und -Zugriff.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die Security Hub-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Security Hub. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Security Hub Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Security Hub verwenden kann, finden Sie unterWie AWS Security Hub funktioniert mit IAM.

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Security Hub zu verwalten. Beispiele für identitätsbasierte Security Hub Hub-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Security Hub

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe

Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.

- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem

Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Anwendungen, die auf Amazon EC2 ausgeführt werden — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und

der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

Wie AWS Security Hub funktioniert mit IAM

Bevor Sie AWS Identity and Access Management den Zugriff auf Security Hub verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen mit Security Hub verwendet werden können.

IAM-Funktionen, die Sie mit Amazon Macie verwenden können

IAM-Feature	Macie-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Nein
Bedingungsschlüssel für die Richtlinie	Ja
Zugriffskontrolllisten (ACLs)	Nein
Attributbasierte Zugriffskontrolle (ABAC) — Tags in Richtlinien	Ja
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Nein

IAM-Feature	Macie-Unterstützung
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie Security Hub und andere mit den meisten IAM-Funktionen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese funktionieren mit IAM.

Identitätsbasierte Richtlinien für Security Hub

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Security Hub unterstützt identitätsbasierte Richtlinien. Weitere Informationen finden Sie unter Beispiele für identitätsbasierte Richtlinien für Security Hub.

Ressourcenbasierte Richtlinien für Security Hub

Unterstützt ressourcenbasierte Richtlinien	Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können

Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Security Hub unterstützt keine ressourcenbasierten Richtlinien. Sie können eine IAM-Richtlinie nicht direkt an eine Security Hub Hub-Ressource anhängen.

Richtlinienaktionen für Security Hub

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Richtlinienaktionen in Security Hub verwenden vor der Aktion das folgende Präfix:

```
securityhub:
```

Um einem Benutzer beispielsweise die Erlaubnis zu erteilen, Security Hub zu aktivieren, was eine Aktion ist, die dem `EnableSecurityHub` Betrieb der Security Hub Hub-API entspricht, nehmen Sie die `securityhub:EnableSecurityHub` Aktion in seine Richtlinie auf. Richtlinienanweisungen müssen entweder ein – `Action`oder ein `NotAction`-Element enthalten. Security Hub definiert eigene Aktionen, die Aufgaben beschreiben, die Sie mit diesem Dienst ausführen können.

```
"Action": "securityhub:EnableSecurityHub"
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata: Beispielsweise:

```
"Action": [
      "securityhub:EnableSecurityHub",
      "securityhub:BatchEnableStandards"
```

Sie können auch mehrere Aktionen mithilfe von Platzhaltern (*) angeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Get` beginnen, einschließlich der folgenden Aktion:

```
"Action": "securityhub:Get*"
```

Als bewährte Methode sollten Sie jedoch Richtlinien erstellen, die dem Prinzip der geringsten Rechte folgen. Mit anderen Worten, Sie sollten Richtlinien erstellen, die nur die Berechtigungen enthalten, die zum Ausführen einer bestimmten Aufgabe erforderlich sind.

Der Benutzer muss Zugriff auf den `DescribeStandardsControl` Vorgang haben, um auf `BatchGetSecurityControlsBatchGetStandardsControlAssociations`, und `ListStandardsControlAssociations` zugreifen zu können.

Der Benutzer muss Zugriff auf den `UpdateStandardsControls` Vorgang haben, um Zugriff auf`BatchUpdateStandardsControlAssociations`, und zu haben`UpdateSecurityControl`.

Eine Liste der Security Hub Hub-Aktionen finden Sie unter Actions defined by AWS Security Hub in der Service Authorization Reference. Beispiele für Richtlinien, die Security Hub Hub-Aktionen spezifizieren, finden Sie unterBeispiele für identitätsbasierte Richtlinien für Security Hub.

Ressourcen

Unterstützt Richtlinienressourcen	Nein

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Security Hub definiert die folgenden Ressourcentypen:

- Hub (Hub)
- Produkt
- Finding-Aggregator, auch als regionsübergreifender Aggregator bezeichnet
- Automatisierungsregel
- Konfigurationsrichtlinie

Sie können diese Ressourcentypen mithilfe von ARNs in Richtlinien angeben.

Eine Liste der Security Hub Hub-Ressourcentypen und der jeweiligen ARN-Syntax finden Sie unter Ressourcentypen definiert von AWS Security Hub in der Service Authorization Reference. Informationen darüber, welche Aktionen Sie für die einzelnen Ressourcentypen angeben können, finden Sie unter Aktionen definiert von AWS Security Hub in der Service Authorization Reference. Beispiele für Richtlinien, die Ressourcen spezifizieren, finden Sie unterBeispiele für identitätsbasierte Richtlinien für Security Hub.

Schlüssel für Richtlinienbedingungen für Security Hub

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der Security Hub Hub-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Security Hub in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Aktionen definiert von AWS Security Hub. Beispiele für Richtlinien, die Bedingungsschlüssel verwenden, finden Sie unterBeispiele für identitätsbasierte Richtlinien für Security Hub.

Zugriffskontrolllisten (ACLs) in Security Hub

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Security Hub unterstützt keine ACLs, was bedeutet, dass Sie keine ACL an eine Security Hub Hub-Ressource anhängen können.

Attributbasierte Zugriffskontrolle (ABAC) mit Security Hub

Unterstützt ABAC (Tags in Richtlinien)	Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Sie können Tags an Security Hub Hub-Ressourcen anhängen. Sie können den Zugriff auf Ressourcen auch kontrollieren, indem Sie Tag-Informationen im `Condition` Element einer Richtlinie angeben.

Informationen zum Taggen von Security Hub Hub-Ressourcen finden Sie unterKennzeichnen von AWS Security Hub Hub-Ressourcen. Ein Beispiel für eine identitätsbasierte Richtlinie, die den

Zugriff auf eine Ressource anhand von Tags steuert, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Security Hub

Temporäre Anmeldeinformationen mit Security Hub verwenden

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS API-Operationen wie AssumeRoleoder aufrufen GetFederationToken.

Security Hub unterstützt die Verwendung temporärer Anmeldeinformationen.

Zugriffssitzungen für Security Hub weiterleiten

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Beispielsweise sendet Security Hub FAS-Anfragen an Downstream, AWS-Services wenn Sie Security Hub in Organizations integrieren AWS Organizations und wenn Sie das delegierte Security Hub-Administratorkonto für eine Organisation festlegen.

Für andere Aufgaben verwendet Security Hub eine dienstbezogene Rolle, um Aktionen in Ihrem Namen auszuführen. Einzelheiten zu dieser Rolle finden Sie unterServiceverknüpfte Rollen für Security Hub.

Servicerollen für Security Hub

Security Hub übernimmt oder verwendet keine Servicerollen. Um Aktionen in Ihrem Namen durchzuführen, verwendet Security Hub eine dienstbezogene Rolle. Einzelheiten zu dieser Rolle finden Sie unterServiceverknüpfte Rollen für Security Hub.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann zu Betriebsproblemen bei Ihrer Nutzung von Security Hub führen. Bearbeiten Sie Servicerollen nur, wenn Security Hub Sie dazu anleitet.

Servicebezogene Rollen für Security Hub

Unterstützt serviceverknüpfte Rollen	Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Security Hub verwendet eine dienstbezogene Rolle, um Aktionen in Ihrem Namen durchzuführen. Einzelheiten zu dieser Rolle finden Sie unterServiceverknüpfte Rollen für Security Hub.

Beispiele für identitätsbasierte Richtlinien für Security Hub

Benutzer und Rollen besitzen standardmäßig keine Berechtigungen zum Erstellen oder Ändern von Security Hub-Ressourcen. Sie können auch keine Aufgaben ausführen, die die AWS Management Console-, – AWS CLIoder AWS-API benutzen. Ein Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den -Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der Security Hub-Konsole
- Beispiel: Erteilen der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Beispiel: Benutzern erlauben, eine Konfigurationsrichtlinie zu erstellen und zu verwalten
- Beispiel: Benutzern erlauben, Ergebnisse anzuzeigen
- Beispiel: Benutzern erlauben, Automatisierungsregeln zu erstellen und zu verwalten

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Security Hub-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS-verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen:Um Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie die AWS-verwaltete Richtlinien die Berechtigungen für viele allgemeine Anwendungsfälle gewähren. Sie sind in Ihrem AWS-Konto verfügbar. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete AWS-Richtlinien

definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien oder AWS-verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.

- Anwendung von Berechtigungen mit den geringsten Rechten:Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs:Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Service-Aktionen zu gewähren, wenn diese durch ein bestimmtes AWS-Service, wie beispielsweise AWS CloudFormation, verwendet werden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten:IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Bedarf einer Multi-Faktor-Authentifizierung (MFA):Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS-Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Security Hub-Konsole

Um auf die AWS Security Hub-Konsole zuzugreifen, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Security Hub-Ressourcen in Ihrem aufzulisten und anzuzeigenAWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Für Benutzer, die nur Aufrufe an die AWS CLI oder AWS-API durchführen, müssen Sie keine Mindestberechtigungen in der Konsole erteilen. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass diese Benutzer und Rollen die Security Hub-Konsole verwenden können, fügen Sie der Entität auch die folgende AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer imIAM-Benutzerhandbuch:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Beispiel: Erteilen der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie enthält Berechtigungen für die Ausführung dieser Aktion auf der Konsole oder für die programmgesteuerte Ausführung über die AWS CLI oder die AWS-API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Beispiel: Benutzern erlauben, eine Konfigurationsrichtlinie zu erstellen und zu verwalten

Dieses Beispiel zeigt, wie Sie eine IAM-Richtlinie erstellen können, die es einem Benutzer ermöglicht, Konfigurationsrichtlinien zu erstellen, anzuzeigen, zu aktualisieren und zu löschen. Diese Beispielrichtlinie ermöglicht es dem Benutzer auch, Richtlinienzuordnungen zu starten, anzuhalten und anzuzeigen. Damit diese IAM-Richtlinie funktioniert, muss der Benutzer der delegierte Security Hub-Administrator für eine Organisation sein.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateConfigurationPolicy",
                "securityhub:UpdateConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetConfigurationPolicy",
                "securityhub:ListConfigurationPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:DeleteConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
```

```
                "securityhub:BatchGetConfigurationPolicyAssociations",
                "securityhub:GetConfigurationPolicyAssociation",
                "securityhub:ListConfigurationPolicyAssociations"
            ],
            "Resource": "*"
        },
        {
            "Sid": "UpdateConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:StartConfigurationPolicyAssociation",
                "securityhub:StartConfigurationPolicyDisassociation"
            ],
            "Resource": "*"
        }
    ]
}
```

Beispiel: Benutzern erlauben, Ergebnisse anzuzeigen

Dieses Beispiel zeigt, wie Sie eine IAM-Richtlinie erstellen können, die es einem Benutzer ermöglicht, Security Hub-Ergebnisse anzuzeigen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

Beispiel: Benutzern erlauben, Automatisierungsregeln zu erstellen und zu verwalten

Dieses Beispiel zeigt, wie Sie eine IAM-Richtlinie erstellen können, die es einem Benutzer ermöglicht, Security Hub-Automatisierungsregeln zu erstellen, anzuzeigen, zu aktualisieren und zu löschen. Damit diese IAM-Richtlinie funktioniert, muss der Benutzer ein Security Hub-

Administrator sein. Um Berechtigungen einzuschränken, z. B. um einem Benutzer nur das Anzeigen von Automatisierungsregeln zu erlauben, können Sie die Berechtigungen zum Erstellen, Aktualisieren und Löschen entfernen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateAutomationRule",
                "securityhub:BatchUpdateAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetAutomationRules",
                "securityhub:ListAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchDeleteAutomationRules"
            ],
            "Resource": "*"
        }
    ]
}
```

Serviceverknüpfte Rollen für Security Hub

AWS Security Hub verwendet eine AWS Identity and Access Management (IAM) serviceverknüpfte Rolle mit dem Namen `AWSServiceRoleForSecurityHub`. Diese serviceverknüpfte Rolle ist eine IAM-Rolle, die direkt mit Security Hub verknüpft ist. Sie wird von Security Hub vordefiniert und umfasst alle Berechtigungen, die Security Hub zum Aufrufen anderer AWS-Services und zur

Überwachung von -AWSRessourcen in Ihrem Namen benötigt. Security Hub verwendet diese serviceverknüpfte Rolle in allen , in AWS-Regionen denen Security Hub verfügbar ist.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von Security Hub, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Security Hub definiert die Berechtigungen seiner serviceverknüpften Rolle. Sofern keine andere Konfiguration festgelegt wurde, kann nur Security Hub die Rolle übernehmen. Die definierten Berechtigungen umfassen die Vertrauensrichtlinie und die Berechtigungsrichtlinie. Sie können diese Berechtigungsrichtlinie keiner anderen IAM-Entität anfügen.

Um die Details der serviceverknüpften Rolle anzuzeigen, wählen Sie auf der Seite Einstellungen der Security Hub-Konsole Allgemein und dann Serviceberechtigungen anzeigen aus.

Sie können die serviceverknüpfte Security Hub-Rolle erst löschen, nachdem Sie Security Hub zum ersten Mal in allen Regionen deaktiviert haben, in denen sie aktiviert ist. Dies schützt Ihre Security Hub-Ressourcen, da Sie nicht versehentlich Berechtigungen für den Zugriff auf sie entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter -AWSServices, die mit IAM funktionieren im IAM-Benutzerhandbuch und suchen Sie die Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Themen

Berechtigungen von serviceverknüpften Rollen für Security Hub

Security Hub verwendet die serviceverknüpfte Rolle namens `AWSServiceRoleForSecurityHub`. Es handelt sich AWS Security Hub um eine serviceverknüpfte Rolle, die für den Zugriff auf Ihre -Ressourcen erforderlich ist. Mit der serviceverknüpften Rolle kann Security Hub Ergebnisse von anderen empfangen AWS-Services und die erforderliche AWS Config Infrastruktur konfigurieren, um Sicherheitsprüfungen für Kontrollen durchzuführen.

Die serviceverknüpfte Rolle `AWSServiceRoleForSecurityHub` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- securityhub.amazonaws.com

Die serviceverknüpfte Rolle AWSServiceRoleForSecurityHub verwendet die verwaltete Richtlinie AWSSecurityHubServiceRolePolicy.

Sie müssen Berechtigungen erteilen, damit eine IAM-Identität (z. B. eine Rolle, Gruppe oder ein Benutzer) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Damit die AWSServiceRoleForSecurityHub serviceverknüpfte Rolle erfolgreich erstellt werden kann, muss die IAM-Identität, die Sie für den Zugriff auf Security Hub verwenden, über die erforderlichen Berechtigungen verfügen. Um die erforderlichen Berechtigungen zu erteilen, fügen Sie die folgende Richtlinie an die Rolle, Gruppe oder den Benutzer an.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Erstellen einer serviceverknüpften Rolle für Security Hub

Die AWSServiceRoleForSecurityHub serviceverknüpfte Rolle wird automatisch erstellt, wenn Sie Security Hub zum ersten Mal aktivieren oder Security Hub in einer unterstützten Region aktivieren, in der Sie sie zuvor nicht aktiviert haben. Sie können die serviceverknüpfte Rolle namens AWSServiceRoleForSecurityHub auch manuell erstellen, indem Sie die IAM-Konsole, die CLI oder die IAM-API verwenden.

> **Important**
>
> Die serviceverknüpfte Rolle, die für das Security Hub-Administratorkonto erstellt wird, gilt nicht für die Security Hub-Mitgliedskonten.

Weitere Informationen zum Erstellen von IAM-Rollen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Bearbeiten einer serviceverknüpften Rolle für Security Hub

Security Hub erlaubt es Ihnen nicht, die `AWSServiceRoleForSecurityHub` serviceverknüpfte Rolle zu bearbeiten. Nachdem Sie eine serviceverknüpfte Rolle erstellt haben, können Sie den Namen der Rolle nicht mehr ändern, da verschiedene Entitäten auf die Rolle verweisen könnten. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Security Hub

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise ist keine ungenutzte Entität vorhanden, die nicht aktiv überwacht oder verwaltet wird.

> **Important**
>
> Um die `AWSServiceRoleForSecurityHub` serviceverknüpfte Rolle zu löschen, müssen Sie zuerst Security Hub in allen Regionen deaktivieren, in denen es aktiviert ist.
> Wenn Security Hub nicht deaktiviert ist, wenn Sie versuchen, die serviceverknüpfte Rolle zu löschen, schlägt das Löschen fehl. Weitere Informationen finden Sie unter Security Hub deaktivieren.

Wenn Sie Security Hub deaktivieren, wird die `AWSServiceRoleForSecurityHub` serviceverknüpfte Rolle nicht automatisch gelöscht. Wenn Sie Security Hub erneut aktivieren, wird die vorhandene `AWSServiceRoleForSecurityHub` serviceverknüpfte Rolle verwendet.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Sie können die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden, um die `AWSServiceRoleForSecurityHub`-serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinien für AWS Security Hub

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Denken Sie daran, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie für alle AWS Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSSecurityHubFullAccess

Sie können die `AWSSecurityHubFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen, die einem Principal vollen Zugriff auf alle Security Hub Hub-Aktionen gewähren. Diese Richtlinie muss einem Prinzipal zugewiesen werden, bevor er Security Hub manuell für sein Konto aktiviert. Principals mit diesen Berechtigungen können beispielsweise den Status der Ergebnisse sowohl einsehen als auch aktualisieren. Sie können benutzerdefinierte Einblicke konfigurieren und Integrationen aktivieren. Sie können Standards und Kontrollen aktivieren und deaktivieren. Principals für ein Administratorkonto können auch Mitgliedskonten verwalten.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `securityhub`— Ermöglicht Principals vollen Zugriff auf alle Security Hub Hub-Aktionen.
- `guardduty`— Ermöglicht Principals, Informationen über den Kontostatus bei Amazon GuardDuty abzurufen.
- `iam`— Ermöglicht Prinzipalen, eine dienstbezogene Rolle zu erstellen.
- `inspector`— Ermöglicht Principals, Informationen zum Kontostatus in Amazon Inspector abzurufen.
- `pricing`— Ermöglicht Principals, eine Preisliste mit Produkten zu erhalten. AWS-Services

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecurityHubAllowAll",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Sid": "SecurityHubServiceLinkedRole",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        },
        {
            "Sid": "OtherServicePermission",
            "Effect": "Allow",
            "Action": [
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "inspector2:BatchGetAccountStatus",
                "pricing:GetProducts"
            ],
            "Resource": "*",
        }
    ]
```

```
}
```

Von Security Hub verwaltete Richtlinie: AWSSecurityHubReadOnlyAccess

Sie können die `AWSSecurityHubReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt nur Leseberechtigungen, die es Benutzern ermöglichen, Informationen in Security Hub einzusehen. Principals, denen diese Richtlinie beigefügt ist, können keine Updates in Security Hub vornehmen. Principals mit diesen Berechtigungen können beispielsweise die mit ihrem Konto verknüpfte Ergebnisliste einsehen, den Status eines Fundes jedoch nicht ändern. Sie können die Ergebnisse von Insights einsehen, aber keine benutzerdefinierten Insights erstellen oder konfigurieren. Sie können keine Steuerungen oder Produktintegrationen konfigurieren.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `securityhub`— Ermöglicht Benutzern das Ausführen von Aktionen, bei denen entweder eine Liste von Elementen oder Details zu einem Artikel zurückgegeben wird. Dazu gehören API-Operationen, die mit `GetList`, oder beginnen`Describe`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSSecurityHubReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "securityhub:Get*",
                "securityhub:List*",
                "securityhub:BatchGet*",
                "securityhub:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS verwaltete Richtlinie: AWSSecurityHubOrganizationsAccess

Sie können die `AWSSecurityHubOrganizationsAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen AWS Organizations , die zur Unterstützung der Security Hub Hub-Integration mit Organizations erforderlich sind.

Diese Berechtigungen ermöglichen es dem Organisationsverwaltungskonto, das delegierte Administratorkonto für Security Hub festzulegen. Sie ermöglichen es dem delegierten Security Hub-Administratorkonto auch, Organisationskonten als Mitgliedskonten zu aktivieren.

Diese Richtlinie stellt nur die Berechtigungen für Organizations bereit. Das Organisationsverwaltungskonto und das delegierte Security Hub-Administratorkonto benötigen ebenfalls Berechtigungen für die zugehörigen Aktionen in Security Hub. Diese Berechtigungen können mithilfe der `AWSSecurityHubFullAccess` verwalteten Richtlinie erteilt werden.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `organizations:ListAccounts`— Ermöglicht Prinzipalen das Abrufen der Liste der Konten, die Teil einer Organisation sind.
- `organizations:DescribeOrganization`— Ermöglicht Prinzipalen das Abrufen von Informationen über die Organisation.
- `organizations:ListRoots`— Ermöglicht Prinzipalen, das Stammverzeichnis einer Organisation aufzulisten.
- `organizations:ListDelegatedAdministrators`— Ermöglicht Prinzipalen, den delegierten Administrator einer Organisation aufzulisten.
- `organizations:ListAWSServiceAccessForOrganization`— Ermöglicht Prinzipalen, diejenigen aufzulisten AWS-Services , die eine Organisation verwendet.
- `organizations:ListOrganizationalUnitsForParent`— Ermöglicht Prinzipalen, die untergeordneten Organisationseinheiten (OU) einer übergeordneten OU aufzulisten.
- `organizations:ListAccountsForParent`— Ermöglicht Prinzipalen, die untergeordneten Konten einer übergeordneten Organisationseinheit aufzulisten.
- `organizations:DescribeAccount`— Ermöglicht Prinzipalen das Abrufen von Informationen über ein Konto in der Organisation.

- `organizations:DescribeOrganizationalUnit`— Ermöglicht Prinzipalen das Abrufen von Informationen über eine Organisationseinheit in der Organisation.
- `organizations:DescribeOrganization`— Ermöglicht Prinzipalen das Abrufen von Informationen über die Organisationskonfiguration.
- `organizations:EnableAWSServiceAccess`— Ermöglicht Prinzipalen, die Security Hub Hub-Integration mit Organizations zu aktivieren.
- `organizations:RegisterDelegatedAdministrator`— Ermöglicht Prinzipalen, das delegierte Administratorkonto für Security Hub festzulegen.
- `organizations:DeregisterDelegatedAdministrator`— Ermöglicht Prinzipalen, das delegierte Administratorkonto für Security Hub zu entfernen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OrganizationPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:ListRoots",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAccountsForParent",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganizationalUnit"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationPermissionsEnable",
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "securityhub.amazonaws.com"
                }
            }
```

```
        },
        {
            "Sid": "OrganizationPermissionsDelegatedAdmin",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator"
            ],
            "Resource": "arn:aws:organizations::*:account/o-*/*",
            "Condition": {
            "StringEquals": {
                "organizations:ServicePrincipal": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

AWS verwaltete Richtlinie: AWSSecurityHubServiceRolePolicy

Sie können `AWSSecurityHubServiceRolePolicy` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es Security Hub ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter the section called “Service-verknüpfte Rollen”.

Diese Richtlinie gewährt Administratorberechtigungen, die es der dienstbezogenen Rolle ermöglichen, die Sicherheitsprüfungen für Security Hub-Steuerelemente durchzuführen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `cloudtrail`— Ruft Informationen über CloudTrail Wanderwege ab.
- `cloudwatch`— Ruft die aktuellen CloudWatch Alarme ab.
- `logs`— Ruft die metrischen Filter für CloudWatch Protokolle ab.
- `sns`— Ruft die Liste der Abonnements für ein SNS-Thema ab.
- `config`— Ruft Informationen zu Konfigurationsrekordern, Ressourcen und AWS Config Regeln ab. Ermöglicht der Rolle, die mit dem Service verknüpft ist, außerdem das Erstellen und Löschen von AWS Config Regeln sowie das Ausführen von Evaluierungen anhand der Regeln.
- `iam`— Abrufen und Generieren von Berichten über Anmeldeinformationen für Konten.

- `organizations`— Rufen Sie Informationen zu Konten und Organisationseinheiten (OU) für eine Organisation ab.
- `securityhub`— Rufen Sie Informationen darüber ab, wie der Security Hub Hub-Dienst, die Standards und die Kontrollen konfiguriert sind.
- `tag`— Ruft Informationen über Ressourcen-Tags ab.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecurityHubServiceRolePermissions",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetEventSelectors",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "logs:DescribeMetricFilters",
                "sns:ListSubscriptionsByTopic",
                "config:DescribeConfigurationRecorders",
                "config:DescribeConfigurationRecorderStatus",
                "config:DescribeConfigRules",
                "config:DescribeConfigRuleEvaluationStatus",
                "config:BatchGetResourceConfig",
                "config:SelectResourceConfig",
                "iam:GenerateCredentialReport",
                "organizations:ListAccounts",
                "config:PutEvaluations",
                "tag:GetResources",
                "iam:GetCredentialReport",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListChildren",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "securityhub:BatchDisableStandards",
                "securityhub:BatchEnableStandards",
                "securityhub:BatchUpdateStandardsControlAssociations",
                "securityhub:BatchGetSecurityControls",
                "securityhub:BatchGetStandardsControlAssociations",
```

```
                "securityhub:CreateMembers",
                "securityhub:DeleteMembers",
                "securityhub:DescribeHub",
                "securityhub:DescribeOrganizationConfiguration",
                "securityhub:DescribeStandards",
                "securityhub:DescribeStandardsControls",
                "securityhub:DisassociateFromAdministratorAccount",
                "securityhub:DisassociateMembers",
                "securityhub:DisableSecurityHub",
                "securityhub:EnableSecurityHub",
                "securityhub:GetEnabledStandards",
                "securityhub:ListStandardsControlAssociations",
                "securityhub:ListSecurityControlDefinitions",
                "securityhub:UpdateOrganizationConfiguration",
                "securityhub:UpdateSecurityControl",
                "securityhub:UpdateSecurityHubConfiguration",
                "securityhub:UpdateStandardsControl",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SecurityHubServiceRoleConfigPermissions",
            "Effect": "Allow",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:GetComplianceDetailsByConfigRule"
            ],
            "Resource": "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
        },
        {
            "Sid": "SecurityHubServiceRoleOrganizationsPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "securityhub.amazonaws.com"
                    ]
                }
```

```
            }
        }
    ]
}
```

Security Hub Hub-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Security Hub an, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Security Hub Hub-Dokumentverlaufsseite.

Änderung	Beschreibung	Datum
AWSSecurityHubFullAccess— Aktualisierung einer bestehenden Richtlinie	Security Hub hat die Richtlinie aktualisiert, um Preisdetails für AWS-Services und Produkte zu erhalten.	24. April 2024
AWSSecurityHubReadOnlyAccess— Aktualisierung einer bestehenden Richtlinie	Security Hub hat diese verwaltete Richtlinie aktualisiert, indem ein `Sid` Feld hinzugefügt wurde.	22. Februar 2024
AWSSecurityHubFullAccess— Aktualisierung einer bestehenden Richtlinie	Security Hub hat die Richtlinie aktualisiert, sodass festgestellt werden kann, ob Amazon GuardDuty und Amazon Inspector in einem Konto aktiviert sind. Auf diese Weise können Kunden sicherheitsrelevante Informationen aus mehreren zusammenführen. AWS-Services	16. November 2023
AWSSecurityHubOrganizationsAccess— Aktualisi	Security Hub hat die Richtlinie aktualisiert, um zusätzlic	16. November 2023

Änderung	Beschreibung	Datum
erung einer bestehenden Richtlinie	he Berechtigungen für den schreibgeschützten Zugriff auf AWS Organizations delegierte Administratorfunkt ionen zu gewähren. Dazu gehören Details wie das Stammverzeichnis, die Organisationseinheiten (OUs), die Konten, die Organisat ionsstruktur und der Servicezu griff.	
AWSSecurityHubServ iceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub hat die `UpdateSecurityCont rol` Berechtigungen `BatchGetSecurityCo ntrols` `Disassoci ateFromAdministrat orAccount` , und zum Lesen und Aktualisieren anpassbarer Sicherhei tskontrolleigenschaften hinzugefügt.	26. November 2023
AWSSecurityHubServ iceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub hat die `tag:GetResources` Berechtigung hinzugefügt, Ressourcen-Tags zu lesen, die sich auf Ergebnisse beziehen.	7. November 2023

Änderung	Beschreibung	Datum
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub hat die `BatchGetStandardsControlAssociations` Erlaubnis hinzugefügt, Informationen über den Aktivierungsstatus eines Steuerelements in einem Standard abzurufen.	27. September 2023
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub hat neue Berechtigungen zum Abrufen von AWS Organizations Daten sowie zum Lesen und Aktualisieren von Security Hub Hub-Konfigurationen, einschließlich Standards und Kontrollen, hinzugefügt.	20. September 2023
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub hat die bestehende `config:DescribeConfigRuleEvaluationStatus` Genehmigung in eine andere Erklärung innerhalb der Richtlinie verschoben. Die `config:DescribeConfigRuleEvaluationStatus` Berechtigung wird jetzt auf alle Ressourcen angewendet.	17. März 2023

Änderung	Beschreibung	Datum
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub hat die bestehende `config:PutEvaluations` Genehmigung in eine andere Erklärung innerhalb der Richtlinie verschoben. Die `config:PutEvaluations` Berechtigung wird jetzt auf alle Ressourcen angewendet.	14. Juli 2021
AWSSecurityHubServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Security Hub hat eine neue Berechtigung hinzugefügt, die es der serviceverknüpften Rolle ermöglicht, Bewertungsergebnisse zu AWS Config liefern.	29. Juni 2021
AWSSecurityHubServiceRolePolicy— Zur Liste der verwalteten Richtlinien hinzugefügt	Es wurden Informationen zur verwalteten Richtlinie hinzugefügt AWSSecurityHubServiceRolePolicy, die von der serviceverknüpften Security Hub Hub-Rolle verwendet wird.	11. Juni 2021
AWSSecurityHubOrganizationsAccess— Neue Richtlinie	Security Hub hat eine neue Richtlinie hinzugefügt, die Berechtigungen gewährt, die für die Security Hub Hub-Integration mit Organizations erforderlich sind.	15. März 2021

Änderung	Beschreibung	Datum
Security Hub hat begonnen, Änderungen zu verfolgen	Security Hub begann, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	15. März 2021

Fehlerbehebung für AWS Security Hub-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Security Hub und IAM auftreten können.

Themen

Ich bin nicht autorisiert, eine Aktion in Security Hub auszuführen

Wenn die AWS Management Console Ihnen mitteilt, dass Sie nicht zur Ausführung einer Aktion autorisiert sind, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Der folgende Beispielfehler tritt auf, wenn der Benutzer `mateojackson` versucht, die Konsole zu verwenden, um Details zu einem *`Widget`* anzuzeigen, aber keine `securityhub:`*`GetWidget`* Berechtigungen hat.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion *`my-example-widget`* auf die Ressource `securityhub:`*`GetWidget`* zugreifen zu können.

Ich bin nicht autorisiert, iam durchzuführen:PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Ausführen der `iam:PassRole` Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an Security Hub übergeben zu können.

Einige AWS-Services erlauben die Übergabe einer vorhandenen Rolle an diesen Dienst, sodass keine neue Servicerolle oder serviceverknüpfte Rolle erstellt werden muss. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Security Hub auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte programmgesteuerten Zugriff auf Security Hub

Benutzer benötigen programmgesteuerten Zugriff, wenn sie außerhalb der AWS Management Console mit AWS interagieren möchten. Die Vorgehensweise, um programmgesteuerten Zugriff zu gewähren, hängt davon ab, welcher Benutzertyp auf zugreift AWS.

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmgesteuerte Anforderungen an die AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
	CLI, AWS-SDKs oder AWS-APIs zu signieren.	• Informationen zur AWS CLI finden Sie unter Konfigurieren der AWS CLI für die Verwendung von AWS IAM Identity Center im AWS Command Line Interface-Benutzerhandbuch. • Informationen zu AWS-SDKs, Tools und AWS-APIs finden Sie unter IAM-Identity-Center-Authentifizierung im Referenzhandbuch zu AWS-SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmgesteuerte Anforderungen an die AWS CLI, AWS-SDKs oder AWS-APIs zu signieren.	Folgen Sie den Anweisungen unter Verwenden temporärer Anmeldeinformationen mit AWS-Ressourcen im IAM-Benutzerhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmgesteuerte Anforderungen an die AWS CLI, AWS-SDKs oder AWS-APIs zu signieren.	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zur AWS CLI finden Sie unter Authentifizierung mit IAM-Benutzer-Anmeldeinformationen im AWS Command Line Interface-Benutzerhandbuch. • Informationen zu AWS-SDKs und Tools finden Sie unter Authentifizierung mit langfristigen Anmeldeinformationen im Referenzhandbuch zu AWS-SDKs und Tools. • Informationen zu AWS-APIs finden Sie unter Verwalten von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch.

Ich bin Administrator und möchte anderen Zugriff auf Security Hub gewähren.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center-Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.

- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine Security Hub-Ressourcen gewähren

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob Security Hub diese Funktionen unterstützt, finden Sie unter Wie AWS Security Hub funktioniert mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konto im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie AWS-Konten-Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter Gewähren des Zugriffs auf AWS-Konten von externen Benutzern im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Compliance-Validierung für AWS Security Hub

Die Auditoren Dritter bewerten die Sicherheit und die Compliance von AWS Security Hub im Rahmen mehrerer AWS-Compliance-Programme. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Eine Liste der AWS-Services, die in den Geltungsbereich bestimmter Compliance-Programme fallen, finden Sie auf der Seite AWS-Services in Scope nach Compliance-Programm. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

Die Auditberichte von Drittanbietern lassen sich mit herunterlade AWS Artifact. Weitere Informationen finden Sie unter Herunterladen von Berichten in AWS Artifact.

Ihre Compliance-Verantwortung bei der Nutzung von Security Hub hängt von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWSstellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung von Vorschriften unterstützen:

- Kurzanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden finden Sie wichtige Überlegungen zur Architektur sowie die einzelnen Schritte zur Bereitstellung von sicherheits- und Compliance-orientierten Basisumgebungen in AWS.
- AWS-Compliance-Ressourcen – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort interessant sein.
- AWS Config – Dieser AWS-Service bewertet, zu welchem Grad die Konfiguration Ihrer Ressourcen den internen Vorgehensweisen, Branchenrichtlinien und Vorschriften entspricht.
- AWS Security Hub – Dieser AWS-Service liefert einen umfassenden Überblick über den Sicherheitsstatus in AWS. So können Sie die Compliance mit den Sicherheitsstandards in der Branche und den bewährten Methoden abgleichen.

Ausfallsicherheit im AWS Security Hub

Im Zentrum der globalen AWS-Infrastruktur stehen die AWS-Regionen und -Availability Zones. Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt.

Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen über AWS-Regionen und Availability Zones finden Sie unter Globale AWS-Infrastruktur.

Sicherheit der Infrastruktur in AWS Security Hub

Als verwalteter Service ist AWS Security Hub durch die globalen Verfahren zur Gewährleistung der Netzwerksicherheit von AWS geschützt. Informationen zu AWS-Sicherheitsservices und wie AWS die Infrastruktur schützt, finden Sie unter AWS-Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Security Hub zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

AWS Security Hub und Schnittstellen-VPC-Endpunkte (AWS PrivateLink)

Sie können eine private Verbindung zwischen Ihrer VPC und AWS Security Hub herstellen, indem Sie einen Schnittstellen-VPC-Endpunkt erstellen. Schnittstellenendpunkte werden von einer Technologie unterstützt AWS PrivateLink, mit der Sie privat auf Security Hub-APIs zugreifen können, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine AWS Direct Connect-Verbindung benötigen. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit Security Hub-APIs zu kommunizieren. Der Datenverkehr zwischen Ihrer VPC und Security Hub verlässt das Amazon-Netzwerk nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic Network-Schnittstellen in Ihren Subnetzen dargestellt.

Weitere Informationen finden Sie im Handbuch unter Interface VPC endpoints (AWS PrivateLink). AWS PrivateLink

Überlegungen zu Security Hub-VPC-Endpunkten

Bevor Sie einen Schnittstellen-VPC-Endpunkt für Security Hub einrichten, stellen Sie sicher, dass Sie die Eigenschaften und Einschränkungen von Schnittstellenendpunkten im AWS PrivateLinkHandbuch überprüfen.

Security Hub unterstützt Aufrufe aller API-Aktionen von Ihrer VPC aus.

> **Note**
>
> Security Hub unterstützt keine VPC-Endpunkte in der Region Asien-Pazifik (Osaka).

Einen VPC-Schnittstellen-Endpunkt für Security Hub erstellen

Sie können einen VPC-Endpunkt für den Security Hub-Dienst entweder mithilfe der Amazon VPC-Konsole oder der AWS Command Line Interface () AWS CLI erstellen. Weitere Informationen finden Sie unter Erstellen eines Schnittstellenendpunkts im AWS PrivateLink-Leitfaden.

Erstellen Sie einen VPC-Endpunkt für Security Hub mit dem folgenden Dienstnamen:

- com.amazonaws.*region*.securityhub

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anfragen an Security Hub stellen, indem Sie beispielsweise seinen Standard-DNS-Namen für die Region verwenden`securityhub.us-east-1.amazonaws.com`.

Weitere Informationen finden Sie im AWS PrivateLinkHandbuch unter Zugreifen auf einen Dienst über einen Schnittstellenendpunkt.

Erstellen einer VPC-Endpunktrichtlinie für Security Hub

Sie können Ihrem VPC-Endpunkt eine Endpunktrichtlinie zuordnen, die den Zugriff auf Security Hub steuert. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie im Handbuch unter Steuern des Zugriffs auf Dienste mit VPC-Endpunkten. AWS PrivateLink

Beispiel: VPC-Endpunktrichtlinie für Security Hub-Aktionen

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für Security Hub. Wenn diese Richtlinie an einen Endpunkt angeschlossen ist, gewährt sie allen Prinzipalen auf allen Ressourcen Zugriff auf die aufgelisteten Security Hub-Aktionen.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

Gemeinsame Subnetze

Sie können VPC-Endpunkte in Subnetzen, die mit Ihnen geteilt werden, nicht erstellen, beschreiben, ändern oder löschen. Sie können die VPC-Endpunkte jedoch in Subnetzen verwenden, die mit Ihnen geteilt werden. Informationen zur VPC-Sharing finden Sie unter Teilen Ihrer VPC mit anderen Konten im Amazon VPC-Benutzerhandbuch.

AWSSecurity Hub Hub-API-Aufrufe protokollieren mit AWS CloudTrail

AWSSecurity Hub ist in einen Dienst integriertAWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in Security Hub ausgeführt wurden. CloudTrail erfasst API-Aufrufe für Security Hub als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Security Hub Hub-Konsole und Code-Aufrufe an die Security Hub Hub-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Security Hub. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem auf der CloudTrail Konsole im Ereignisverlauf einsehen. Anhand der CloudTrail gesammelten Informationen können Sie die Anfrage, die an Security Hub gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen darüber CloudTrail, einschließlich der Konfiguration und Aktivierung, finden Sie im AWS CloudTrailBenutzerhandbuch.

Security Hub Hub-Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviertAWS-Konto, wenn Sie das Konto erstellen. Wenn unterstützte Ereignisaktivitäten in Security Hub auftreten, wird diese Aktivität zusammen mit anderen AWS Dienstereignissen im CloudTrail Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können die neusten Ereignisse in Ihr -Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung von Ereignissen in Ihrem Konto, einschließlich Ereignissen für Security Hub, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Standardmäßig gilt ein in der Konsole erstellter Trail für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails

- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Security Hub unterstützt die Protokollierung aller Security Hub Hub-API-Aktionen als Ereignisse in CloudTrail Protokollen. Eine Liste der Security Hub Hub-Operationen finden Sie in der Security Hub Hub-API-Referenz.

Wenn Aktivitäten für die folgenden Aktionen protokolliert werden CloudTrail, `responseElements` ist der Wert für auf gesetzt`null`. Dadurch wird sichergestellt, dass vertrauliche Informationen nicht in den CloudTrail Protokollen enthalten sind.

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM)-Benutzer-Anmeldeinformationen ausgeführt wurde.
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde
- Ob die Anforderung von einem anderen AWS-Service getätigt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Beispiel: Einträge in der Security Hub Hub-Protokolldatei

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen

oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `CreateInsight` Aktion demonstriert. In diesem Beispiel wird ein Insight mit dem Namen `Test Insight` erstellt. Das `ResourceId` Attribut ist als Gruppieren nach Aggregator angegeben, und es wurden keine optionalen Filter für diesen Einblick angegeben. Weitere Informationen über Funde sind unter Einblicke in AWS Security Hub verfügbar.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJK6U5DS22IAVUI7BW",
        "arn": "arn:aws:iam::012345678901:user/TestUser",
        "accountId": "012345678901",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "TestUser"
    },
    "eventTime": "2018-11-25T01:02:18Z",
    "eventSource": "securityhub.amazonaws.com",
    "eventName": "CreateInsight",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
    "requestParameters": {
        "Filters": {},
        "ResultField": "ResourceId",
        "Name": "Test Insight"
    },
    "responseElements": {
        "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/
f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
    },
    "requestID": "c0fffccd-f04d-11e8-93fc-ddcd14710066",
    "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "012345678901"
}
```

Kennzeichnen von AWS Security Hub Hub-Ressourcen

Ein Tag ist eine optionale Bezeichnung, die Sie definieren und AWS Ressourcen zuweisen können, einschließlich bestimmter Typen von AWS Security Hub Hub-Ressourcen. Mithilfe von Tags können Sie Ressourcen auf unterschiedliche Weise identifizieren, kategorisieren und verwalten, z. B. nach Zweck, Eigentümer, Umgebung oder anderen Kriterien. Mithilfe von Tags können Sie beispielsweise zwischen Ressourcen unterscheiden, Ressourcen identifizieren, die bestimmte Compliance-Anforderungen oder Workflows unterstützen, oder Kosten zuordnen.

Sie können den folgenden Typen von Security Hub Hub-Ressourcen Tags zuweisen: Automatisierungsregeln, Konfigurationsrichtlinien und die Hub Ressource.

Themen

Grundlagen der Kennzeichnung

Eine Ressource kann bis zu 50 Tags enthalten. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert. Beides können Sie definieren. Ein Tag-Schlüssel ist eine allgemeine Bezeichnung, die als Kategorie für einen spezifischeren Tag-Wert dient. Ein Tag-Wert dient als Bezeichnung für einen Tag-Schlüssel.

Wenn Sie beispielsweise unterschiedliche Automatisierungsregeln für verschiedene Umgebungen erstellen (einen Satz von Automatisierungsregeln für Testkonten und einen anderen für Produktionskonten), können Sie diesen Regeln einen `Environment` Tagschlüssel zuweisen. Der zugehörige Tagwert kann `Test` für die Regeln gelten, die Testkonten zugeordnet sind, und `Prod` für die Regeln, die Produktionskonten und Organisationseinheiten zugeordnet sind.

Beachten Sie bei der Definition und Zuweisung von Tags zu AWS Security Hub Hub-Ressourcen Folgendes:

- Jede Ressource kann maximal 50 Tags haben.
- Für jede Ressource muss jeder Tag-Schlüssel eindeutig sein und er kann nur einen Tag-Wert haben.
- Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden. Als bewährte Methode empfehlen wir Ihnen, eine Strategie zur Großschreibung von Tags zu definieren und diese Strategie in allen Ressourcen einheitlich umzusetzen.
- Ein Tag-Schlüssel kann maximal 128 UTF-8-Zeichen enthalten. Ein Tag-Wert kann maximal 256 UTF-8-Zeichen enthalten. Die Zeichen können Buchstaben, Zahlen, Leerzeichen oder die folgenden Symbole sein: _.:/= + - @
- Das `aws:` Präfix ist für die Verwendung durch reserviertAWS. Sie können es nicht in Tag-Schlüsseln oder -Werten verwenden, die Sie definieren. Außerdem können Sie Tag-Schlüssel oder Werte, die dieses Präfix verwenden, nicht ändern oder entfernen. Tags mit diesem Präfix werden beim Kontingent von 50 Tags pro Ressource nicht eingerechnet.
- Alle Tags, die Sie zuweisen, sind nur für Sie AWS-Konto und nur in dem verfügbar, AWS-Region in dem Sie sie zuweisen.
- Wenn Sie einer Ressource mithilfe von Security Hub Tags zuweisen, werden die Tags nur auf die Ressource angewendet, die direkt in Security Hub im entsprechenden Verzeichnis gespeichert istAWS-Region. Sie gelten nicht für zugehörige, unterstützende Ressourcen, die Security Hub für Sie in anderen Bereichen erstellt, verwendet oder verwaltetAWS-Services. Wenn Sie beispielsweise einer Automatisierungsregel, die Ergebnisse im Zusammenhang mit Amazon Simple Storage Service (Amazon S3) aktualisiert, Tags zuweisen, werden die Tags nur auf Ihre Automatisierungsregel in Security Hub für die angegebene Region angewendet. Sie werden nicht auf Ihre S3-Buckets angewendet. Um auch einer zugehörigen Ressource Tags zuzuweisen, können Sie AWS Resource Groups oder das verwenden, AWS-Service das die Ressource speichert — zum Beispiel Amazon S3 für einen S3-Bucket. Das Zuweisen von Tags zu zugehörigen Ressourcen kann Ihnen dabei helfen, unterstützende Ressourcen für Ihre Security Hub Hub-Ressourcen zu identifizieren.
- Wenn Sie eine Ressource löschen, werden alle Tags, die der Ressource zugewiesen sind, ebenfalls gelöscht.

> **Important**
>
> Speichern Sie keine vertraulichen oder anderen sensiblen Daten in Tags. Auf Tags kann von vielen aus zugegriffen werdenAWS-Services, darunterAWS Billing and Cost Management. Sie sind nicht dafür vorgesehen, für sensible Daten verwendet zu werden.

Um Tags für Security Hub Hub-Ressourcen hinzuzufügen und zu verwalten, können Sie die Security Hub Hub-Konsole, die Security Hub Hub-API oder die AWS Resource Groups Tagging-API verwenden. Mit Security Hub können Sie einer Ressource Tags hinzufügen, wenn Sie die Ressource erstellen. Sie können auch Tags für einzelne vorhandene Ressourcen hinzufügen und verwalten. Mit Resource Groups können Sie Tags für mehrere bestehende RessourcenAWS-Services, einschließlich Security Hub, in großen Mengen hinzufügen und verwalten.

Weitere Tipps und bewährte Methoden zur Kennzeichnung finden Sie unter Tagging Your AWS Resources User Guide im Tagging AWS Resources User Guide.

Verwenden von Tags in IAM-Richtlinien

Nachdem Sie mit dem Taggen von Ressourcen begonnen haben, können Sie tagbasierte Berechtigungen auf Ressourcenebene in (IAM-) Richtlinien definieren. AWS Identity and Access Management Durch die Verwendung von Tags auf diese Weise können Sie detailliert steuern, welche Benutzer und Rollen in Ihrem Unternehmen die Berechtigung AWS-Konto haben, Ressourcen zu erstellen und zu taggen, und welche Benutzer und Rollen generell die Berechtigung haben, Tags hinzuzufügen, zu bearbeiten und zu entfernen. Um den Zugriff anhand von Tags zu steuern, können Sie im Element Condition der IAM-Richtlinien Tag-bezogene Bedingungsschlüssel verwenden.

Sie können beispielsweise eine IAM-Richtlinie erstellen, die einem Benutzer vollen Zugriff auf alle AWS Security Hub-Ressourcen gewährt, wenn das `Owner` Tag für die Ressource seinen Benutzernamen angibt:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*",
```

```
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Wenn Sie Tag-basierte Berechtigungen auf Ressourcenebene definieren, werden die Berechtigungen sofort wirksam. Dies bedeutet, dass Ihre Ressourcen besser geschützt sind, sobald sie erstellt wurden, und Sie schnell damit beginnen können, die Verwendung von Tags für neue Ressourcen zu erzwingen. Mithilfe von Berechtigungen auf Ressourcenebene können Sie auch steuern, welche Tag-Schlüssel und -Werte können mit neuen und vorhandenen Ressourcen verknüpft werden können. Weitere Informationen finden Sie unter Steuern des Zugriffs auf AWS-Ressourcen mithilfe von Tags im IAM-Benutzerhandbuch.

Hinzufügen von Tags zu AWS Security Hub Hub-Ressourcen

Um einer einzelnen AWS Security Hub Hub-Ressource Tags hinzuzufügen, können Sie die Security Hub Hub-Konsole oder die Security Hub Hub-API verwenden. Die Konsole unterstützt das Hinzufügen von Tags zur Hub Ressource nicht.

Um mehreren Security Hub Hub-Ressourcen gleichzeitig Tags hinzuzufügen, verwenden Sie die Tagging-Operationen der AWS Resource GroupsTagging-API.

> **Important**
>
> Das Hinzufügen von Tags zu einer Ressource kann sich auf den Zugriff auf die Ressource auswirken. Bevor Sie einer Ressource ein Tag hinzufügen, überprüfen Sie alle AWS Identity and Access Management (IAM-) Richtlinien, die möglicherweise Tags verwenden, um den Zugriff auf Ressourcen zu steuern.

Console

So fügen Sie einer Ressource einen Tag hinzu

Wenn Sie eine Automatisierungsregel oder eine Konfigurationsrichtlinie erstellen, bietet die Security Hub Hub-Konsole Optionen zum Hinzufügen von Tags. Sie können den Tag-Schlüssel und den Tag-Wert im Abschnitt Tags angeben.

Security Hub API & AWS CLI

So fügen Sie einer Ressource einen Tag hinzu

Um eine Ressource zu erstellen und ihr programmgesteuert ein oder mehrere Tags hinzuzufügen, verwenden Sie den entsprechenden Vorgang für den Ressourcentyp, den Sie erstellen möchten:

- Um eine Konfigurationsrichtlinie zu erstellen und ihr ein oder mehrere Tags hinzuzufügen, rufen Sie die CreateConfigurationPolicyAPI auf oder führen Sie, falls Sie die verwendenAWS CLI, den Befehl aus. create-configuration-policy
- Um eine Automatisierungsregel zu erstellen und ihr ein oder mehrere Tags hinzuzufügen, rufen Sie die CreateAutomationRuleAPI auf oder führen Sie, falls Sie die verwendenAWS CLI, den create-automation-ruleBefehl aus.
- Um Security Hub zu aktivieren und Ihrer Hub Ressource ein oder mehrere Tags hinzuzufügen, rufen Sie die EnableSecurityHubAPI auf oder führen Sie, falls Sie die AWS Command Line Interface (AWS CLI) verwenden, den enable-security-hubBefehl aus.

Verwenden Sie in Ihrer Anfrage den `tags` Parameter, um den Tag-Schlüssel und den optionalen Tag-Wert für jedes Tag anzugeben, das der Ressource hinzugefügt werden soll. Der `tags` Parameter gibt ein Array von Objekten an. Jedes Objekt gibt einen Tag-Schlüssel und den zugehörigen Tag-Wert an.

Um einer vorhandenen Ressource ein oder mehrere Tags hinzuzufügen, verwenden Sie den TagResourceBetrieb der Security Hub Hub-API oder, falls Sie die verwendenAWS CLI, führen Sie den Befehl tag-resource aus. Geben Sie in Ihrer Anfrage den Amazon-Ressourcennamen (ARN) der Ressource an, der Sie ein Tag hinzufügen möchten. Verwenden Sie den `tags` Parameter, um den Tag-Schlüssel (`key`) und den optionalen Tag-Wert (`value`) für jedes hinzuzufügende Tag anzugeben. Der `tags` Parameter gibt ein Array von Objekten an, ein Objekt für jeden Tag-Schlüssel und den zugehörigen Tag-Wert.

Der folgende AWS CLI Befehl fügt beispielsweise der angegebenen Konfigurationsrichtlinie einen `Prod` Tag-Schlüssel mit einem Tag-Wert hinzu. `Environment` Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\), um die Lesbarkeit zu verbessern.

Beispiel für einen CLI-Befehl:

```
$ aws securityhub tag-resource \
```

```
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Prod
```

Wobei gilt:

- `resource-arn`gibt den ARN der Konfigurationsrichtlinie an, zu der ein Tag hinzugefügt werden soll.
- *`Environment`*ist der Tag-Schlüssel des Tags, das der Regel hinzugefügt werden soll.
- *`Prod`*ist der Tag-Wert für den angegebenen Tag-Schlüssel (*`Environment`*).

Im folgenden Beispiel fügt der Befehl der Konfigurationsrichtlinie mehrere Tags hinzu.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Prod key=CostCenter,value=12345 key=Owner,value=jane-
doe
```

Für jedes Objekt in einem `tags` Array sind `key` sowohl die `value` Argumente als auch erforderlich. Der Wert für das `value` Argument kann jedoch eine leere Zeichenfolge sein. Wenn Sie einem Tag-Schlüssel keinen Tag-Wert zuordnen möchten, geben Sie keinen Wert für das `value` Argument an. Mit dem folgenden Befehl wird beispielsweise ein `Owner` Tag-Schlüssel ohne zugehörigen Tag-Wert hinzugefügt:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Owner,value=
```

Wenn ein Tagging-Vorgang erfolgreich ist, gibt Security Hub eine leere HTTP 200-Antwort zurück. Andernfalls gibt Security Hub eine HTTP 4 xx - oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Tags für AWS Security Hub Hub-Ressourcen überprüfen

Sie können die Tags (sowohl Tag-Schlüssel als auch Tag-Werte) für eine Security Hub Hub-Automatisierungsregel oder -konfigurationsrichtlinie mithilfe der Security Hub Hub-Konsole oder der

Security Hub Hub-API überprüfen. Die Konsole unterstützt die Überprüfung von Tags für die Hub Ressource nicht.

Verwenden Sie die Tagging-Operationen der Tagging-API, um Tags für mehrere Security Hub Hub-Ressourcen gleichzeitig zu überprüfen. AWS Resource Groups

Console

Um die Tags für eine Ressource zu überprüfen

1. Öffnen Sie mit den Anmeldeinformationen des Security Hub-Administrators die AWS Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/.
2. Gehen Sie je nach Art der Ressource, der Sie ein Tag hinzufügen möchten, wie folgt vor:
   - Um die Tags für eine Automatisierungsregel zu überprüfen, wählen Sie im Navigationsbereich Automatisierungen aus. Wählen Sie dann eine Automatisierungsregel aus.
   - Um die Tags für eine Konfigurationsrichtlinie zu überprüfen, wählen Sie im Navigationsbereich Konfiguration aus. Wählen Sie dann auf der Registerkarte Richtlinien die Option neben einer Konfigurationsrichtlinie aus. Ein Seitenbereich wird geöffnet, in dem die Anzahl der der Richtlinie zugewiesenen Tags angezeigt wird. Sie können den Tags-Header erweitern, um die Tag-Schlüssel und Tag-Werte zu sehen.

Im Abschnitt „Tags“ werden alle Tags aufgeführt, die der Ressource derzeit zugewiesen sind.

Security Hub API & AWS CLI

Um die Tags für eine Ressource zu überprüfen

Rufen Sie die ListTagsForResourceAPI auf, um die Tags für eine vorhandene Ressource abzurufen und zu überprüfen. Verwenden Sie in Ihrer Anfrage den `resourceArn` Parameter, um den Amazon-Ressourcennamen (ARN) der Ressource anzugeben.

Wenn Sie den verwendenAWS CLI, führen Sie den list-tags-for-resourceBefehl aus und geben Sie mit dem `resource-arn` Parameter den ARN der Ressource an. Beispiel:

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Wenn der Vorgang erfolgreich ist, gibt Security Hub ein `tags` Array zurück. Jedes Objekt im Array spezifiziert ein Tag (sowohl den Tag-Schlüssel als auch den Tag-Wert), das der Ressource aktuell zugewiesen ist. Beispiel:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Prod"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

Wobei `EnvironmentCostCenter`, und `Owner` die Tag-Schlüssel sind, die der Ressource zugewiesen sind. `Prod`ist der Tag-Wert, der dem `Environment` Tag-Schlüssel zugeordnet ist. `12345`ist der Tag-Wert, der dem `CostCenter` Tag-Schlüssel zugeordnet ist. Dem `Owner` Tag-Schlüssel ist kein Tag-Wert zugeordnet.

Um eine Liste aller Security Hub Hub-Ressourcen mit Tags und aller Tags, die jeder dieser Ressourcen zugewiesen sind, abzurufen, verwenden Sie den GetResourcesBetrieb der AWS Resource Groups Tagging-API. Setzen Sie in Ihrer Anfrage den Wert für den `ResourceTypeFilters` Parameter auf`securityhub`. Führen Sie dazu mit dem den AWS CLI Befehl get-resources aus und setzen Sie den Wert für den `resource-type-filters` Parameter auf`securityhub`. Beispiel:

```
$ aws resourcegroupstaggingapi get-resources -\-resource-type-filters "securityhub"
```

Wenn der Vorgang erfolgreich ist, gibt Resource Groups ein `ResourceTagMappingList` Array zurück. Das Array enthält ein Objekt für jede Security Hub Hub-Ressource, die über Tags verfügt. Jedes Objekt spezifiziert den ARN einer Security Hub Hub-Ressource sowie die Tag-Schlüssel und -Werte, die der Ressource zugewiesen sind.

Tags für AWS Security Hub Hub-Ressourcen bearbeiten

Um Tags (Tag-Schlüssel oder Tag-Werte) für eine AWS Security Hub Hub-Ressource zu bearbeiten, können Sie die Security Hub Hub-API verwenden. Die Security Hub Hub-Konsole unterstützt derzeit keine Tag-Bearbeitung.

Um Tags für mehrere Security Hub Hub-Ressourcen gleichzeitig zu bearbeiten, verwenden Sie die Tagging-Operationen der AWS Resource GroupsTagging-API.

> **Important**
>
> Die Bearbeitung der Tags für eine Ressource kann sich auf den Zugriff auf die Ressource auswirken. Bevor Sie einen Tag-Schlüssel oder -Wert für eine Ressource bearbeiten, sollten Sie alle AWS Identity and Access Management (IAM-) Richtlinien überprüfen, die das Tag möglicherweise zur Steuerung des Zugriffs auf Ressourcen verwenden.

Security Hub API & AWS CLI

Um die Tags für eine Ressource zu bearbeiten

Wenn Sie ein Tag für eine Ressource programmgesteuert bearbeiten, überschreiben Sie das vorhandene Tag mit neuen Werten. Daher hängt die beste Methode zum Bearbeiten eines Tags davon ab, ob Sie einen Tag-Schlüssel, einen Tag-Wert oder beides bearbeiten möchten. Um einen Tag-Schlüssel zu bearbeiten, entfernen Sie das aktuelle Tag und fügen Sie ein neues Tag hinzu.

Um nur den Tag-Wert zu bearbeiten oder zu entfernen, der einem Tag-Schlüssel zugeordnet ist, überschreiben Sie den vorhandenen Wert mithilfe TagResourceder Security Hub Hub-API. Wenn Sie den verwendenAWS CLI, führen Sie den Befehl tag-resource aus. Geben Sie in Ihrer Anfrage den Amazon-Ressourcennamen (ARN) der Ressource an, deren Tag-Wert Sie bearbeiten oder entfernen möchten.

Um einen Tag-Wert zu bearbeiten, verwenden Sie den `tags` Parameter, um den Tag-Schlüssel anzugeben, dessen Tag-Wert Sie ändern möchten. Sie sollten auch den neuen Tag-Wert für den Schlüssel angeben. Mit dem folgenden AWS CLI Befehl wird beispielsweise der Tag-Wert `Test` für `Prod` den `Environment` Tag-Schlüssel, der der angegebenen Automatisierungsregel zugewiesen ist, von auf geändert. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\), um die Lesbarkeit zu verbessern.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Test
```

Wobei gilt:

- `resource-arn`gibt den ARN der Konfigurationsrichtlinie an.
- *`Environment`*ist der Tag-Schlüssel, der dem zu ändernden Tag-Wert zugeordnet ist.
- *`Test`*ist der neue Tag-Wert für den angegebenen Tag-Schlüssel (*`Environment`*).

Um einen Tag-Wert aus einem Tag-Schlüssel zu entfernen, geben Sie im `tags` Parameter keinen Wert für das `value` Argument des Schlüssels an. Beispiel:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Owner,value=
```

Wenn der Vorgang erfolgreich ist, gibt Security Hub eine leere HTTP 200-Antwort zurück. Andernfalls gibt Security Hub eine HTTP 4 xx - oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Tags aus AWS Security Hub Hub-Ressourcen entfernen

Um Tags aus einer AWS Security Hub Hub-Ressource zu entfernen, können Sie die Security Hub Hub-API verwenden. Die Security Hub Hub-Konsole unterstützt derzeit das Entfernen von Tags nicht.

Um Tags aus mehreren Security Hub Hub-Ressourcen gleichzeitig zu entfernen, verwenden Sie die Tagging-Operationen der AWS Resource GroupsTagging-API.

> **Important**
>
> Das Entfernen von Tags aus einer Ressource kann sich auf den Zugriff auf die Ressource auswirken. Bevor Sie ein Tag entfernen, überprüfen Sie alle AWS Identity and Access Management (IAM-) Richtlinien, die das Tag möglicherweise zur Steuerung des Zugriffs auf Ressourcen verwenden.

Security Hub API & AWS CLI

Um Tags aus einer Ressource zu entfernen

Um ein oder mehrere Tags programmgesteuert aus einer Ressource zu entfernen, verwenden Sie den UntagResourceBetrieb der Security Hub Hub-API. Verwenden Sie in Ihrer Anfrage den `resourceArn` Parameter, um den Amazon-Ressourcennamen (ARN) der Ressource anzugeben, aus der ein Tag entfernt werden soll. Verwenden Sie den `tagKeys` Parameter, um den Tag-Schlüssel des Tags anzugeben, das entfernt werden soll. Um mehrere Tags zu entfernen, hängen Sie den `tagKeys` Parameter und das Argument für jedes zu entfernende Tag an, getrennt durch ein Und-Zeichen (&) — zum Beispiel. `tagKeys=`*`key1`*`&tagKeys=`*`key2`* Um nur einen bestimmten Tag-Wert (keinen Tag-Schlüssel) aus einer Ressource zu entfernen, bearbeiten Sie das Tag, anstatt das Tag zu entfernen.

Wenn Sie den verwendenAWS CLI, führen Sie den Befehl untag-resource aus, um ein oder mehrere Tags aus einer Ressource zu entfernen. Geben Sie für den `resource-arn` Parameter den ARN der Ressource an, aus der ein Tag entfernt werden soll. Verwenden Sie den `tag-keys` Parameter, um den Tag-Schlüssel des Tags anzugeben, das entfernt werden soll. Mit dem folgenden Befehl wird beispielsweise das `Environment` Tag (sowohl der Tag-Schlüssel als auch der Tag-Wert) aus der angegebenen Konfigurationsrichtlinie entfernt:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

Where `resource-arn` gibt den ARN der Konfigurationsrichtlinie an, aus der ein Tag entfernt werden soll, und *`Environment`* ist der Tag-Schlüssel des Tags, aus dem entfernt werden soll.

Um mehrere Tags aus einer Ressource zu entfernen, fügen Sie jeden zusätzlichen Tag-Schlüssel als Argument für den `tag-keys` Parameter hinzu. Beispiel:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

Wenn der Vorgang erfolgreich ist, gibt Security Hub eine leere HTTP 200-Antwort zurück. Andernfalls gibt Security Hub eine HTTP 4 xx - oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Security Hub Hub-Kontingente

Ihr AWS-Konto hat für jedes Kontingent bestimmte Standardkontingente, früher als Limits bezeichnetAWS-Service. Diese Kontingente sind die maximale Anzahl von Serviceressourcen oder Vorgängen für Ihr Konto. Dieses Thema enthält Links zu den Kontingenten, die für AWS Security Hub Hub-Ressourcen und -Vorgänge für Ihr Konto gelten. Sofern nicht anders angegeben, gilt jedes Kontingent jeweils für Ihr KontoAWS-Region.

Einige Kontingente können erhöht werden, andere dagegen nicht. Verwenden Sie die Service Quotas-Konsole, um eine Erhöhung eines Kontingents anzufordern. Informationen dazu, wie Sie eine Erhöhung beantragen können, finden Sie unter Eine Erhöhung des Kontingents beantragen im Benutzerhandbuch zu Service Quotas. Wenn ein Kontingent in der Service-Kontingents-Konsole nicht verfügbar ist, verwenden Sie das Formular zur Erhöhung des Servicelimits auf derAWS Support Center Console, um eine Erhöhung des Kontingents zu beantragen.

Maximale Kontingente

Eine Liste der Kontingente, die für Security Hub Hub-Ressourcen gelten, finden Sie unter AWSSecurity Hub Hub-Endpunkte und Kontingente in der Allgemeine AWS-Referenz.

Ratenkontingente

Eine Liste der Kontingente, die für Security Hub Hub-API-Operationen gelten, finden Sie in der AWSSecurity Hub Hub-API-Referenz.

Wenn Sie einen Aufruf eingerichtet habenRegionsübergreifende Aggregation, `BatchUpdateFindings` wirkt sich dies auf verknüpfte Regionen und die Aggregationsregion aus. `BatchImportFindings` Der `GetFindings` Vorgang ruft Ergebnisse aus verknüpften Regionen und der Aggregationsregion ab. Die `UpdateStandardsControl` Operationen `BatchEnableStandards` und sind jedoch regionsspezifisch.

Security Hub — Regionale Beschränkungen

Einige AWS Security Hub Hub-Funktionen sind nur in bestimmten Fällen verfügbar AWS-Regionen. In den folgenden Abschnitten werden diese regionalen Beschränkungen beschrieben.

Eine Liste der Regionen, in denen Security Hub verfügbar ist, finden Sie unter AWS Security Hub Hub-Endpunkte und Kontingente in der Allgemeine AWS-Referenz.

Regionsübergreifende Aggregationsbeschränkungen

In AWS GovCloud (US) ist die regionsübergreifende Aggregation nur für Ergebnisse, Suchaktualisierungen und Erkenntnisse verfügbar. AWS GovCloud (US) Insbesondere können Sie nur Ergebnisse, Aktualisierungen und Erkenntnisse zwischen AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) zusammenfassen.

In den Regionen Chinas ist die regionsübergreifende Aggregation nur für Ergebnisse, Suchaktualisierungen und Erkenntnisse aus den Regionen China verfügbar. Insbesondere können Sie Ergebnisse, Aktualisierungen und Erkenntnisse nur zwischen China (Peking) und China (Ningxia) zusammenfassen.

Sie können eine Region, die standardmäßig deaktiviert ist, nicht als Ihre Aggregationsregion verwenden. Eine Liste der Regionen, die standardmäßig deaktiviert sind, finden Sie unter Aktivieren einer Region in der Allgemeine AWS-Referenz.

Verfügbarkeit von Integrationen nach Regionen

Einige Integrationen sind in allen Regionen nicht verfügbar. Wenn eine Integration in einer bestimmten Region nicht verfügbar ist, wird sie nicht auf der Seite Integrationen der Security Hub Hub-Konsole aufgeführt, wenn Sie diese Region auswählen.

Integrationen, die in China (Peking) und China (Ningxia) unterstützt werden

Die Regionen China (Peking) und China (Ningxia) unterstützen nur die folgenden Integrationen mit Diensten: AWS

- AWS Firewall Manager
- Amazon GuardDuty

- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer
- AWS Systems Manager OpsCenter
- AWS Systems Manager Patch-Manager

Die Regionen China (Peking) und China (Ningxia) unterstützen nur die folgenden Integrationen von Drittanbietern:

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar
- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler
- RSA Archer
- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

Integrationen, die in AWS GovCloud (US-Ost) und (US-West) unterstützt werden AWS GovCloud

Die Regionen AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) unterstützen nur die folgenden Integrationen mit Diensten: AWS

- AWS Config
- Amazon Detective
- AWS Firewall Manager

- Amazon GuardDuty
- AWS Health
- IAM Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender

Die Regionen AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) unterstützen nur die folgenden Integrationen von Drittanbietern:

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud
- Atlassian OpsGenie
- Caveonix Cloud
- Cloud Custodian
- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB
- Forcepoint DLP
- Forcepoint NGFW
- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator
- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series(nur in AWS GovCloud (US-West) verfügbar)
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect

- RSA Archer
- SecureCloudDb
- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

Verfügbarkeit von Standards nach Regionen

Service-Managed Standard: AWS Control Tower ist nur in Regionen verfügbar, in denen AWS Control Tower Folgendes unterstützt wird: AWS GovCloud (US) Eine Liste der Regionen, die dies AWS Control Tower unterstützen, finden Sie unter How AWS-Regionen Work With AWS Control Tower im AWS Control Tower Benutzerhandbuch.

Der AWS Resource Tagging Standard ist in Kanada West (Calgary), China und nicht verfügbar. AWS GovCloud (US)

Andere Sicherheitsstandards sind in allen Regionen verfügbar, in denen Security Hub verfügbar ist.

Verfügbarkeit von Kontrollen nach Regionen

Security Hub-Steuerelemente sind möglicherweise nicht in allen Regionen verfügbar. Eine Liste der nicht verfügbaren Steuerelemente in den einzelnen Regionen finden Sie unterRegionale Grenzwerte für Kontrollen. Ein Steuerelement erscheint nicht in der Liste der Steuerelemente in der Security Hub Hub-Konsole, wenn es in der Region, in der Sie angemeldet sind, nicht verfügbar ist. Die Ausnahme ist, wenn Sie in einer Aggregationsregion angemeldet sind. In diesem Fall können Sie Steuerelemente sehen, die in der Aggregationsregion oder in einer oder mehreren verknüpften Regionen verfügbar sind.

Regionale Grenzwerte für Kontrollen

AWS Security Hub-Steuerelemente sind möglicherweise nicht in allen verfügbar AWS-Regionen. Auf dieser Seite wird angezeigt, welche Steuerelemente in bestimmten Regionen nicht verfügbar sind. Ein Steuerelement erscheint nicht in der Liste der Steuerelemente in der Security Hub Hub-Konsole, wenn es in der Region, in der Sie angemeldet sind, nicht verfügbar ist. Die Ausnahme ist, wenn Sie in

einer Aggregationsregion angemeldet sind. In diesem Fall können Sie Steuerelemente sehen, die in der Aggregationsregion oder in einer oder mehreren verknüpften Regionen verfügbar sind.

Inhalt

- Naher Osten (Bahrain)
- Naher Osten (VAE)
- Südamerika (São Paulo)
- AWS GovCloud (US-Ost)
- AWS GovCloud (US-West)

USA Ost (Nord-Virginia)

Die folgenden Steuerelemente werden in USA Ost (Nord-Virginia) nicht unterstützt.

- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [ElastiCache.4] ElastiCache für Redis-Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache für Redis-Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache Für Redis-Replikationsgruppen vor Version 6.0 sollte Redis AUTH verwendet werden
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben

- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden

USA Ost (Ohio)

Die folgenden Steuerelemente werden in US East (Ohio) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein

- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

USA West (Nordkalifornien)

Die folgenden Steuerelemente werden in USA West (Nordkalifornien) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein

- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben

- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

USA West (Oregon)

Die folgenden Steuerelemente werden in US West (Oregon) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden

- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Afrika (Kapstadt)

Die folgenden Steuerelemente werden in Afrika (Kapstadt) nicht unterstützt.

- [ACM.1] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ApiGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben

- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden

- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.3] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.12] Ungenutzte Amazon EC2 EC2-EIPs sollten entfernt werden
- [EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen
- [EC2.14] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulassen
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden
- [ELB.2] Classic Load Balancer mit SSL/HTTPS-Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.4] Application Load Balancer sollte so konfiguriert sein, dass HTTP-Header gelöscht werden
- [ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config

- [ELB.16] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden
- [IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden
- [IoT.3] AWS IoT Core -Dimensionen sollten markiert werden
- [IoT.4] AWS IoT Core Autorisierer sollten markiert werden
- [IoT.5] AWS IoT Core Rollenaliase sollten markiert werden
- [IoT.6] AWS IoT Core Richtlinien sollten markiert werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein
- Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein

- [Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben
- Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.9] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.10] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

- [WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein

Asien-Pazifik (Hongkong)

Die folgenden Steuerelemente werden im asiatisch-pazifischen Raum (Hongkong) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen

- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.10] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein

- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Asien-Pazifik (Hyderabad)

Die folgenden Steuerelemente werden im asiatisch-pazifischen Raum (Hyderabad) nicht unterstützt.

- [ACM.1] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [Account.2] AWS-Konten sollte Teil einer Organisation sein AWS Organizations
- [ApiGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein
- [ApiGateway.2] API Gateway REST-API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [ApiGateway.3] Bei den REST-API-Stufen von API Gateway sollte die Ablaufverfolgung aktiviert sein AWS X-Ray
- [ApiGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein
- [ApiGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben
- [ApiGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden

- [Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden
- [Athena.3] Athena-Arbeitsgruppen sollten markiert werden
- [AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden
- [Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.3] AWS Backup Tresore sollten markiert sein
- [Backup.4] AWS Backup Berichtspläne sollten markiert werden
- [Backup.5] AWS Backup Backup-Pläne sollten markiert werden
- [CloudFormation.2] CloudFormation Stapel sollten markiert werden
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist

- [CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild1.4] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [Detective.1] Verhaltensdiagramme von Detektiven sollten markiert werden
- [DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
- [DMS.2] DMS-Zertifikate sollten gekennzeichnet sein
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen

- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen
- [EC2.14] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulassen
- [EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen
- [EC2.22] Ungenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.34] Die Routentabellen des EC2-Transit-Gateways sollten mit Tags versehen werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.48] Amazon VPC-Flow-Logs sollten markiert werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen

- [EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen
- [EFS.5] EFS-Zugangspunkte sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [ELB.5] Die Protokollierung von Anwendungen und Classic Load Balancers sollte aktiviert sein
- [ELB.13] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ElastiCache.1] Bei ElastiCache Redis-Clustern sollte das automatische Backup aktiviert sein
- [ElastiCache.6] ElastiCache Für Redis-Replikationsgruppen vor Version 6.0 sollte Redis AUTH verwendet werden
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [ES.1] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein
- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein
- [EventBridge.2] EventBridge Eventbusse sollten gekennzeichnet sein
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden

- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [Glue.1] AWS Glue Jobs sollten markiert werden
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen werden
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden
- [IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden
- [IoT.3] AWS IoT Core -Dimensionen sollten markiert werden
- [IoT.4] AWS IoT Core Autorisierer sollten markiert werden

- [IoT.5] AWS IoT Core Rollenaliase sollten markiert werden
- [IoT.6] AWS IoT Core Richtlinien sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben

- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein
- Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben
- Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch -Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.2] RDS-DB-Instances sollten je nach Dauer den öffentlichen Zugriff verbieten PubliclyAccessible AWS Config
- [RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein
- [RDS.9] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.16] RDS-DB-Cluster sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden

- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.28] RDS-DB-Cluster sollten markiert werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein
- [Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten
- [Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden
- [Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein
- [Redshift.6] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein
- [Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten
- [S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [SNS.3] SNS-Themen sollten markiert werden

- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [Transfer.1] AWS Transfer Family -Workflows sollten mit Tags versehen werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein

Asien-Pazifik (Jakarta)

Die folgenden Steuerelemente werden im asiatisch-pazifischen Raum (Jakarta) nicht unterstützt.

- [Account.2] AWS-Konten sollte Teil einer Organisation sein AWS Organizations
- [ApiGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein
- [ApiGateway.2] API Gateway REST-API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden

- [ApiGateway.3] Bei den REST-API-Stufen von API Gateway sollte die Ablaufverfolgung aktiviert sein AWS X-Ray
- [ApiGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein
- [ApiGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben
- [ApiGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen
- [AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden
- [AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden
- [Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.4] AWS Backup Berichtspläne sollten markiert werden
- [Backup.5] AWS Backup Backup-Pläne sollten markiert werden
- [CloudFormation.2] CloudFormation Stapel sollten markiert werden
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln

- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild1.4] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [Detective.1] Verhaltensdiagramme von Detektiven sollten markiert werden
- [DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
- [DMS.2] DMS-Zertifikate sollten gekennzeichnet sein
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein

- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen
- [EC2.14] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulassen
- [EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen
- [EC2.22] Ungenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECS.2] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden

- [ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen
- [ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden
- [ECS.5] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein
- [ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [ECS.10] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen
- [ECS.12] ECS-Cluster sollten Container Insights verwenden
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [ELB.12] Application Load Balancer sollte mit dem defensiven Modus oder dem strengsten Modus zur Desynchronisierung konfiguriert werden
- [ELB.13] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ElastiCache.1] Bei ElastiCache Redis-Clustern sollte das automatische Backup aktiviert sein
- [ElastiCache.6] ElastiCache Für Redis-Replikationsgruppen vor Version 6.0 sollte Redis AUTH verwendet werden
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben

- [ES.1] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein
- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [Glue.1] AWS Glue Jobs sollten markiert werden
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen werden
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden
- [IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden
- [IoT.3] AWS IoT Core -Dimensionen sollten markiert werden
- [IoT.4] AWS IoT Core Autorisierer sollten markiert werden
- [IoT.5] AWS IoT Core Rollenaliase sollten markiert werden
- [IoT.6] AWS IoT Core Richtlinien sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein

- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein
- Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben
- Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.9] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch

- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.16] RDS-DB-Cluster sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten
- [Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden
- [Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein
- [Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden
- [Redshift.9] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [S3.11] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein
- [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [SNS.3] SNS-Themen sollten markiert werden
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden

- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein

Asien-Pazifik (Mumbai)

Die folgenden Steuerelemente werden im asiatisch-pazifischen Raum (Mumbai) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten

- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein

- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Asien-Pazifik (Melbourne)

Die folgenden Steuerelemente werden im asiatisch-pazifischen Raum (Melbourne) nicht unterstützt.

- [ACM.1] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [ApiGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein
- [ApiGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben
- [ApiGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.4] AWS AppSync GraphQL-APIs sollten markiert werden
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden
- [Athena.3] Athena-Arbeitsgruppen sollten markiert werden
- [AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden
- [Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben

- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.3] AWS Backup Tresore sollten markiert sein
- [Backup.4] AWS Backup Berichtspläne sollten markiert werden
- [Backup.5] AWS Backup Backup-Pläne sollten markiert werden
- [CloudFormation.2] CloudFormation Stapel sollten markiert werden
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild1.4] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben

- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [Detective.1] Verhaltensdiagramme von Detektiven sollten markiert werden
- [DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
- [DMS.2] DMS-Zertifikate sollten gekennzeichnet sein
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.1] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein

- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.9] Amazon EC2 EC2-Instances sollten keine öffentliche IPv4-Adresse haben
- [EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen
- [EC2.14] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulassen
- [EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen
- [EC2.22] Ungenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.33] EC2 Transit Gateway-Anhänge sollten markiert werden
- [EC2.34] Die Routentabellen des EC2-Transit-Gateways sollten mit Tags versehen werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.48] Amazon VPC-Flow-Logs sollten markiert werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.52] EC2-Transit-Gateways sollten markiert werden
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen

- [EFS.5] EFS-Zugangspunkte sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [EKS.6] EKS-Cluster sollten markiert werden
- [EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden
- [EKS.8] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein
- [ELB.13] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ElastiCache.1] Bei ElastiCache Redis-Clustern sollte das automatische Backup aktiviert sein
- [ElastiCache.2] ElastiCache Für Redis-Cache-Cluster sollte das auto Upgrade der Nebenversion aktiviert sein
- [ElastiCache.3] ElastiCache Für Redis-Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache für Redis-Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache für Redis-Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache Für Redis-Replikationsgruppen vor Version 6.0 sollte Redis AUTH verwendet werden
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [ES.1] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein

- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein
- [EventBridge.2] EventBridge Eventbusse sollten gekennzeichnet sein
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [Glue.1] AWS Glue Jobs sollten markiert werden
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen werden
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen
- [IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.
- [IAM.7] Die Passwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.10] Passwortrichtlinien für IAM-Benutzer sollten strenge Laufzeiten haben AWS Config
- [IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert
- [IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert
- [IAM.13] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist
- [IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert

- [IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
- [IAM.16] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert
- [IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden
- [IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden
- [IoT.3] AWS IoT Core -Dimensionen sollten markiert werden
- [IoT.4] AWS IoT Core Autorisierer sollten markiert werden
- [IoT.5] AWS IoT Core Rollenaliase sollten markiert werden
- [IoT.6] AWS IoT Core Richtlinien sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch

- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

- Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein
- Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben
- Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch -Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.
- [RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein
- [RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.16] RDS-DB-Cluster sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.28] RDS-DB-Cluster sollten markiert werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein
- [Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein

- [S3.15] Bei S3-Allzweck-Buckets sollte Object Lock aktiviert sein
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [SNS.1] SNS-Themen sollten im Ruhezustand wie folgt verschlüsselt werden AWS KMS
- [SNS.3] SNS-Themen sollten markiert werden
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [StepFunctions.2] Die Aktivitäten von Step Functions sollten markiert werden
- [Transfer.1] AWS Transfer Family -Workflows sollten mit Tags versehen werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

- [WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein

Asien-Pazifik (Osaka)

Die folgenden Steuerelemente werden im asiatisch-pazifischen Raum (Osaka) nicht unterstützt.

- [ACM.1] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [Account.2] AWS-Konten sollte Teil einer Organisation sein AWS Organizations
- [ApiGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein
- [ApiGateway.2] API Gateway REST-API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [ApiGateway.3] Bei den REST-API-Stufen von API Gateway sollte die Ablaufverfolgung aktiviert sein AWS X-Ray
- [ApiGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein
- [Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein
- [Backup.4] AWS Backup Berichtspläne sollten markiert werden
- [CloudFormation.2] CloudFormation Stapel sollten markiert werden
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln

- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CloudWatch.15] Für CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein
- [CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild1.4] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [Detective.1] Verhaltensdiagramme von Detektiven sollten markiert werden
- [DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen

- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.2] Bei DynamoDB-Tabellen sollte die Wiederherstellung aktiviert sein point-in-time
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.1] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein
- [EC2.3] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein
- [EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.9] Amazon EC2 EC2-Instances sollten keine öffentliche IPv4-Adresse haben
- [EC2.10] Amazon EC2 sollte so konfiguriert sein, dass es VPC-Endpunkte verwendet, die für den Amazon EC2-Service erstellt wurden
- [EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen
- [EC2.14] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulassen
- [EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen
- [EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden
- [EC2.17] Amazon EC2 EC2-Instances sollten nicht mehrere ENIs verwenden
- [EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen
- [EC2.20] Beide VPN-Tunnel für eine AWS Site-to-Site-VPN-Verbindung sollten aktiv sein
- [EC2.22] Ungenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden

- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.52] EC2-Transit-Gateways sollten markiert werden
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.
- [ECS.2] ECS-Diensten sollten nicht automatisch öffentliche IP-Adressen zugewiesen werden
- [ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen
- [ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden
- [ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [ECS.10] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen
- [ECS.12] ECS-Cluster sollten Container Insights verwenden
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden
- [ELB.2] Classic Load Balancer mit SSL/HTTPS-Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden
- [ELB.4] Application Load Balancer sollte so konfiguriert sein, dass HTTP-Header gelöscht werden
- [ELB.6] Für Anwendungen, Gateways und Network Load Balancers sollte der Löschschutz aktiviert sein

- [ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config
- [ELB.9] Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein
- [ELB.16] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF
- [ElastiCache.1] Bei ElastiCache Redis-Clustern sollte das automatische Backup aktiviert sein
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [ES.1] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein
- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden
- [IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden
- [IoT.3] AWS IoT Core -Dimensionen sollten markiert werden
- [IoT.4] AWS IoT Core Autorisierer sollten markiert werden
- [IoT.5] AWS IoT Core Rollenaliase sollten markiert werden

- [IoT.6] AWS IoT Core Richtlinien sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.3] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden
- [Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten
- [Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden
- [Lambda.3] Lambda-Funktionen sollten sich in einer VPC befinden
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein
- Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben

- Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.4] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden
- [RDS.6] Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden
- [RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein
- [RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein
- [RDS.9] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.10] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden
- [RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden
- [RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein
- [Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten
- [Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden
- [Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein
- [Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren
- [S3.15] Bei S3-Allzweck-Buckets sollte Object Lock aktiviert sein

- [S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SecretsManager.1] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein
- [SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren
- [SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen
- [SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [SNS.1] SNS-Themen sollten im Ruhezustand wie folgt verschlüsselt werden AWS KMS
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein

Asien-Pazifik (Seoul)

Die folgenden Steuerelemente werden im asiatisch-pazifischen Raum (Seoul) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden

- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Asien-Pazifik (Singapur)

Die folgenden Steuerelemente werden im asiatisch-pazifischen Raum (Singapur) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein

- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein

- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Asien-Pazifik (Sydney)

Die folgenden Steuerelemente werden im asiatisch-pazifischen Raum (Sydney) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden

- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben

- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Asien-Pazifik (Tokio)

Die folgenden Steuerelemente werden im asiatisch-pazifischen Raum (Tokio) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden

- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Kanada (Zentral)

Die folgenden Steuerelemente werden in Kanada (Central) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein

- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch

- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

China (Peking)

Die folgenden Steuerelemente werden in China (Peking) nicht unterstützt.

- [ACM.1] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [ACM.3] ACM-Zertifikate sollten mit einem Tag versehen werden
- [Account.2] AWS-Konten sollte Teil einer Organisation sein AWS Organizations
- [ApiGateway.2] API Gateway REST-API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [ApiGateway.3] Bei den REST-API-Stufen von API Gateway sollte die Ablaufverfolgung aktiviert sein AWS X-Ray

- [ApiGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein
- [AppSync.4] AWS AppSync GraphQL-APIs sollten markiert werden
- [Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden
- [Athena.3] Athena-Arbeitsgruppen sollten markiert werden
- [AutoScaling.10] EC2 Auto Scaling Scaling-Gruppen sollten markiert werden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.3] AWS Backup Tresore sollten markiert sein
- [Backup.4] AWS Backup Berichtspläne sollten markiert werden
- [Backup.5] AWS Backup Backup-Pläne sollten markiert werden
- [CloudFormation.2] CloudFormation Stapel sollten markiert werden
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CloudTrail.9] CloudTrail Pfade sollten markiert werden
- [CloudWatch.15] Für CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein
- [CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden

- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [Detective.1] Verhaltensdiagramme von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten gekennzeichnet sein
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.5] DynamoDB-Tabellen sollten mit Tags versehen werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen
- [EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden
- [EC2.20] Beide VPN-Tunnel für eine AWS Site-to-Site-VPN-Verbindung sollten aktiv sein
- [EC2.22] Ungenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden

- [EC2.33] EC2 Transit Gateway-Anhänge sollten markiert werden
- [EC2.34] Die Routentabellen des EC2-Transit-Gateways sollten mit Tags versehen werden
- [EC2.35] EC2-Netzwerkschnittstellen sollten markiert werden
- [EC2.36] EC2-Kunden-Gateways sollten mit Tags versehen werden
- [EC2.37] EC2-Elastic-IP-Adressen sollten mit Tags versehen werden
- [EC2.38] EC2-Instances sollten markiert werden
- [EC2.39] EC2-Internet-Gateways sollten markiert werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.41] EC2-Netzwerk-ACLs sollten markiert werden
- [EC2.42] EC2-Routing-Tabellen sollten mit Tags versehen werden
- [EC2.43] EC2-Sicherheitsgruppen sollten markiert werden
- [EC2.44] EC2-Subnetze sollten markiert werden
- [EC2.45] EC2-Volumes sollten markiert werden
- [EC2.46] Amazon VPCs sollten markiert werden
- [EC2.47] Amazon VPC Endpoint Services sollten markiert werden
- [EC2.48] Amazon VPC-Flow-Logs sollten markiert werden
- [EC2.49] Amazon VPC-Peering-Verbindungen sollten markiert werden
- [EC2.50] EC2-VPN-Gateways sollten markiert werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.52] EC2-Transit-Gateways sollten markiert werden
- [EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 zu Remote-Serververwaltungsports zulassen
- [EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugang von: :/0 zu Remote-Serveradministrationsports zulassen
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.
- [ECS.13] ECS-Services sollten markiert werden
- [ECS.14] ECS-Cluster sollten markiert werden

- [ECS.15] ECS-Aufgabendefinitionen sollten mit Tags versehen werden
- [EFS.5] EFS-Zugangspunkte sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [EKS.6] EKS-Cluster sollten markiert werden
- [EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden
- [ELB.2] Classic Load Balancer mit SSL/HTTPS-Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.16] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF
- [ElastiCache.1] Bei ElastiCache Redis-Clustern sollte das automatische Backup aktiviert sein
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.2] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein
- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein
- [ES.9] Elasticsearch-Domains sollten markiert werden
- [EventBridge.2] EventBridge Eventbusse sollten gekennzeichnet sein
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [Glue.1] AWS Glue Jobs sollten markiert werden
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen werden
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.

- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.23] IAM Access Analyzer-Analyzer sollten markiert werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IAM.28] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein
- [IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden
- [IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden
- [IoT.3] AWS IoT Core -Dimensionen sollten markiert werden
- [IoT.4] AWS IoT Core Autorisierer sollten markiert werden
- [IoT.5] AWS IoT Core Rollenaliase sollten markiert werden
- [IoT.6] AWS IoT Core Richtlinien sollten markiert werden
- [Kinesis.2] Kinesis-Streams sollten markiert werden
- [Lambda.6] Lambda-Funktionen sollten markiert werden
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren

- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.7] Netzwerk-Firewall-Firewalls sollten markiert werden
- [NetworkFirewall.8] Firewall-Richtlinien für Netzwerk-Firewalls sollten markiert werden
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein
- Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben
- Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch -Domains sollten mit Tags versehen werden
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [PCA.1] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein
- [RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein
- [RDS.10] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden
- [RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden

- [RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.16] RDS-DB-Cluster sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.28] RDS-DB-Cluster sollten markiert werden
- [RDS.29] RDS-DB-Cluster-Snapshots sollten mit Tags versehen werden
- [RDS.30] RDS-DB-Instances sollten markiert werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.32] RDS-DB-Snapshots sollten markiert werden
- [RDS.33] RDS-DB-Subnetzgruppen sollten markiert werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein
- [Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.11] Redshift-Cluster sollten markiert werden
- [Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden
- [Redshift.13] Redshift-Cluster-Snapshots sollten markiert werden
- [Redshift.14] Redshift-Cluster-Subnetzgruppen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein
- [S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren

- [S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein
- [S3.22] S3-Allzweck-Buckets sollten Schreibereignisse auf Objektebene protokollieren
- [S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen
- [SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden
- [SecretsManager.5] Secrets Manager Manager-Geheimnisse sollten markiert werden
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [SNS.3] SNS-Themen sollten markiert werden
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [StepFunctions.2] Die Aktivitäten von Step Functions sollten markiert werden
- [Transfer.1] AWS Transfer Family -Workflows sollten mit Tags versehen werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein

China (Ningxia)

Die folgenden Steuerelemente werden in China (Ningxia) nicht unterstützt.

- [ACM.1] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [ACM.3] ACM-Zertifikate sollten mit einem Tag versehen werden
- [Account.2] AWS-Konten sollte Teil einer Organisation sein AWS Organizations
- [ApiGateway.2] API Gateway REST-API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [ApiGateway.3] Bei den REST-API-Stufen von API Gateway sollte die Ablaufverfolgung aktiviert sein AWS X-Ray
- [ApiGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein
- [AppSync.4] AWS AppSync GraphQL-APIs sollten markiert werden
- [Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden
- [Athena.3] Athena-Arbeitsgruppen sollten markiert werden
- [AutoScaling.10] EC2 Auto Scaling Scaling-Gruppen sollten markiert werden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.3] AWS Backup Tresore sollten markiert sein
- [Backup.4] AWS Backup Berichtspläne sollten markiert werden
- [Backup.5] AWS Backup Backup-Pläne sollten markiert werden
- [CloudFormation.2] CloudFormation Stapel sollten markiert werden
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln

- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CloudTrail.9] CloudTrail Pfade sollten markiert werden
- [CloudWatch.15] Für CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein
- [CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [Detective.1] Verhaltensdiagramme von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten gekennzeichnet sein
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.5] DynamoDB-Tabellen sollten mit Tags versehen werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen
- [EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden
- [EC2.20] Beide VPN-Tunnel für eine AWS Site-to-Site-VPN-Verbindung sollten aktiv sein

- [EC2.22] Ungenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.33] EC2 Transit Gateway-Anhänge sollten markiert werden
- [EC2.34] Die Routentabellen des EC2-Transit-Gateways sollten mit Tags versehen werden
- [EC2.35] EC2-Netzwerkschnittstellen sollten markiert werden
- [EC2.36] EC2-Kunden-Gateways sollten mit Tags versehen werden
- [EC2.37] EC2-Elastic-IP-Adressen sollten mit Tags versehen werden
- [EC2.38] EC2-Instances sollten markiert werden
- [EC2.39] EC2-Internet-Gateways sollten markiert werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.41] EC2-Netzwerk-ACLs sollten markiert werden
- [EC2.42] EC2-Routing-Tabellen sollten mit Tags versehen werden
- [EC2.43] EC2-Sicherheitsgruppen sollten markiert werden
- [EC2.44] EC2-Subnetze sollten markiert werden
- [EC2.45] EC2-Volumes sollten markiert werden
- [EC2.46] Amazon VPCs sollten markiert werden
- [EC2.47] Amazon VPC Endpoint Services sollten markiert werden
- [EC2.48] Amazon VPC-Flow-Logs sollten markiert werden
- [EC2.49] Amazon VPC-Peering-Verbindungen sollten markiert werden
- [EC2.50] EC2-VPN-Gateways sollten markiert werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.52] EC2-Transit-Gateways sollten markiert werden
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.
- [ECS.13] ECS-Services sollten markiert werden

- [ECS.14] ECS-Cluster sollten markiert werden
- [ECS.15] ECS-Aufgabendefinitionen sollten mit Tags versehen werden
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen
- [EFS.5] EFS-Zugangspunkte sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [EKS.6] EKS-Cluster sollten markiert werden
- [EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden
- [ELB.2] Classic Load Balancer mit SSL/HTTPS-Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.16] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF
- [ElastiCache.1] Bei ElastiCache Redis-Clustern sollte das automatische Backup aktiviert sein
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.2] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein
- [ES.1] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein
- [ES.9] Elasticsearch-Domains sollten markiert werden
- [EventBridge.2] EventBridge Eventbusse sollten gekennzeichnet sein
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [Glue.1] AWS Glue Jobs sollten markiert werden
- [GuardDuty.1] GuardDuty sollte aktiviert sein

- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen werden
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.23] IAM Access Analyzer-Analyzer sollten markiert werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IAM.28] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein
- [IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden
- [IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden
- [IoT.3] AWS IoT Core -Dimensionen sollten markiert werden
- [IoT.4] AWS IoT Core Autorisierer sollten markiert werden
- [IoT.5] AWS IoT Core Rollenaliase sollten markiert werden
- [IoT.6] AWS IoT Core Richtlinien sollten markiert werden
- [Kinesis.2] Kinesis-Streams sollten markiert werden
- [Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten
- [Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden
- [Lambda.3] Lambda-Funktionen sollten sich in einer VPC befinden
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Lambda.6] Lambda-Funktionen sollten markiert werden
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [MQ.4] Amazon MQ-Broker sollten markiert werden

- [Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.7] Netzwerk-Firewall-Firewalls sollten markiert werden
- [NetworkFirewall.8] Firewall-Richtlinien für Netzwerk-Firewalls sollten markiert werden
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein
- Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben
- Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch -Domains sollten mit Tags versehen werden
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [PCA.1] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein
- [RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein
- [RDS.9] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.10] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden

- [RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden
- [RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.28] RDS-DB-Cluster sollten markiert werden
- [RDS.29] RDS-DB-Cluster-Snapshots sollten mit Tags versehen werden
- [RDS.30] RDS-DB-Instances sollten markiert werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.32] RDS-DB-Snapshots sollten markiert werden
- [RDS.33] RDS-DB-Subnetzgruppen sollten markiert werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein
- [Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein
- [Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.11] Redshift-Cluster sollten markiert werden
- [Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden
- [Redshift.13] Redshift-Cluster-Snapshots sollten markiert werden
- [Redshift.14] Redshift-Cluster-Subnetzgruppen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein
- [S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren

- [S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen
- [SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden
- [SecretsManager.5] Secrets Manager Manager-Geheimnisse sollten markiert werden
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [SNS.3] SNS-Themen sollten markiert werden
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [StepFunctions.2] Die Aktivitäten von Step Functions sollten markiert werden
- [Transfer.1] AWS Transfer Family -Workflows sollten mit Tags versehen werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein

Europa (Frankfurt)

Die folgenden Steuerelemente werden in Europa (Frankfurt) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein

- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Europa (Irland)

Die folgenden Steuerelemente werden in Europa (Irland) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein

- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch

- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Europa (London)

Die folgenden Steuerelemente werden in Europa (London) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln

- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein

- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Europa (Milan)

Die folgenden Steuerelemente werden in Europa (Mailand) nicht unterstützt.

- [ACM.1] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ApiGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen

- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.3] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.12] Ungenutzte Amazon EC2 EC2-EIPs sollten entfernt werden
- [EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen
- [EC2.14] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulassen
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECS.12] ECS-Cluster sollten Container Insights verwenden
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden

- [ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden
- [ELB.2] Classic Load Balancer mit SSL/HTTPS-Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.4] Application Load Balancer sollte so konfiguriert sein, dass HTTP-Header gelöscht werden
- [ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config
- [ELB.16] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden
- [IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden
- [IoT.3] AWS IoT Core -Dimensionen sollten markiert werden
- [IoT.4] AWS IoT Core Autorisierer sollten markiert werden
- [IoT.5] AWS IoT Core Rollenaliase sollten markiert werden
- [IoT.6] AWS IoT Core Richtlinien sollten markiert werden
- [KMS.3] AWS KMS keys sollte nicht unbeabsichtigt gelöscht werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein

- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein
- Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben
- Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.4] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden
- [RDS.9] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden
- [Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein

- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein

Europa (Paris)

Die folgenden Steuerelemente werden in Europa (Paris) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein

- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben

- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Europa (Spain)

Die folgenden Steuerelemente werden in Europa (Spanien) nicht unterstützt.

- [ACM.1] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [Account.2] AWS-Konten sollte Teil einer Organisation sein AWS Organizations
- [ApiGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein
- [ApiGateway.2] API Gateway REST-API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [ApiGateway.3] Bei den REST-API-Stufen von API Gateway sollte die Ablaufverfolgung aktiviert sein AWS X-Ray
- [ApiGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein

- [ApiGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben
- [ApiGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden
- [Athena.3] Athena-Arbeitsgruppen sollten markiert werden
- [AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden
- [Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.3] AWS Backup Tresore sollten markiert sein
- [Backup.4] AWS Backup Berichtspläne sollten markiert werden
- [Backup.5] AWS Backup Backup-Pläne sollten markiert werden
- [CloudFormation.2] CloudFormation Stapel sollten markiert werden
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen

- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist
- [CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist
- [CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild1.4] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [Detective.1] Verhaltensdiagramme von Detektiven sollten markiert werden
- [DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
- [DMS.2] DMS-Zertifikate sollten gekennzeichnet sein
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein

- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.1] DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren
- [DynamoDB.2] Bei DynamoDB-Tabellen sollte die Wiederherstellung aktiviert sein point-in-time
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.1] Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein
- [EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen
- [EC2.3] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein
- [EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein
- [EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.9] Amazon EC2 EC2-Instances sollten keine öffentliche IPv4-Adresse haben
- [EC2.10] Amazon EC2 sollte so konfiguriert sein, dass es VPC-Endpunkte verwendet, die für den Amazon EC2-Service erstellt wurden
- [EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen
- [EC2.14] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulassen
- [EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen

- [EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden
- [EC2.17] Amazon EC2 EC2-Instances sollten nicht mehrere ENIs verwenden
- [EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen
- [EC2.20] Beide VPN-Tunnel für eine AWS Site-to-Site-VPN-Verbindung sollten aktiv sein
- [EC2.22] Ungenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.34] Die Routentabellen des EC2-Transit-Gateways sollten mit Tags versehen werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.48] Amazon VPC-Flow-Logs sollten markiert werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen
- [EFS.5] EFS-Zugangspunkte sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden

- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden
- [ELB.2] Classic Load Balancer mit SSL/HTTPS-Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden
- [ELB.4] Application Load Balancer sollte so konfiguriert sein, dass HTTP-Header gelöscht werden
- [ELB.5] Die Protokollierung von Anwendungen und Classic Load Balancers sollte aktiviert sein
- [ELB.6] Für Anwendungen, Gateways und Network Load Balancers sollte der Löschschutz aktiviert sein
- [ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config
- [ELB.9] Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.16] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF
- [ElastiCache.1] Bei ElastiCache Redis-Clustern sollte das automatische Backup aktiviert sein
- [ElastiCache.6] ElastiCache Für Redis-Replikationsgruppen vor Version 6.0 sollte Redis AUTH verwendet werden
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [ES.1] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein
- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden

- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein
- [EventBridge.2] EventBridge Eventbusse sollten gekennzeichnet sein
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [Glue.1] AWS Glue Jobs sollten markiert werden
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen werden
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden

- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden
- [IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden
- [IoT.3] AWS IoT Core -Dimensionen sollten markiert werden
- [IoT.4] AWS IoT Core Autorisierer sollten markiert werden
- [IoT.5] AWS IoT Core Rollenaliase sollten markiert werden
- [IoT.6] AWS IoT Core Richtlinien sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.4] Die AWS KMS Schlüsselrotation sollte aktiviert sein
- [Lambda.1] Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten
- [Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden
- [Lambda.3] Lambda-Funktionen sollten sich in einer VPC befinden
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein

- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein
- Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben
- Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch -Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben

- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.2] RDS-DB-Instances sollten je nach Dauer den öffentlichen Zugriff verbieten PubliclyAccessible AWS Config
- [RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.
- [RDS.4] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden
- [RDS.5] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden
- [RDS.6] Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden
- [RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein
- [RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein
- [RDS.9] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch
- [RDS.10] Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden
- [RDS.11] Bei RDS-Instances sollten automatische Backups aktiviert sein
- [RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden
- [RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.16] RDS-DB-Cluster sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.28] RDS-DB-Cluster sollten markiert werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein
- [Redshift.1] Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten
- [Redshift.2] Verbindungen zu Amazon Redshift Redshift-Clustern sollten bei der Übertragung verschlüsselt werden
- [Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein
- [Redshift.6] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein

- [Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein
- [S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern
- [S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten
- [S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren
- [S3.9] Bei S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein
- [S3.15] Bei S3-Allzweck-Buckets sollte Object Lock aktiviert sein
- [S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [SNS.1] SNS-Themen sollten im Ruhezustand wie folgt verschlüsselt werden AWS KMS
- [SNS.3] SNS-Themen sollten markiert werden
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden

- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [Transfer.1] AWS Transfer Family -Workflows sollten mit Tags versehen werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein

Europa (Stockholm)

Die folgenden Steuerelemente werden in Europa (Stockholm) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein

- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden

- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Europa (Zürich)

Die folgenden Steuerelemente werden in Europa (Zürich) nicht unterstützt.

- [ACM.1] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden

- [ApiGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein
- [ApiGateway.2] API Gateway REST-API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [ApiGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben
- [ApiGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden
- [Athena.3] Athena-Arbeitsgruppen sollten markiert werden
- [AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden
- [Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.3] AWS Backup Tresore sollten markiert sein
- [Backup.4] AWS Backup Berichtspläne sollten markiert werden
- [Backup.5] AWS Backup Backup-Pläne sollten markiert werden
- [CloudFormation.2] CloudFormation Stapel sollten markiert werden
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln

- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist
- [CloudTrail.7] Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild1.4] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [Detective.1] Verhaltensdiagramme von Detektiven sollten markiert werden
- [DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
- [DMS.2] DMS-Zertifikate sollten gekennzeichnet sein
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden

- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.1] DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren
- [DynamoDB.2] Bei DynamoDB-Tabellen sollte die Wiederherstellung aktiviert sein point-in-time
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen
- [EC2.3] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein
- [EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.9] Amazon EC2 EC2-Instances sollten keine öffentliche IPv4-Adresse haben
- [EC2.10] Amazon EC2 sollte so konfiguriert sein, dass es VPC-Endpunkte verwendet, die für den Amazon EC2-Service erstellt wurden
- [EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen
- [EC2.14] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulassen
- [EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen

- [EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden
- [EC2.17] Amazon EC2 EC2-Instances sollten nicht mehrere ENIs verwenden
- [EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen
- [EC2.20] Beide VPN-Tunnel für eine AWS Site-to-Site-VPN-Verbindung sollten aktiv sein
- [EC2.22] Ungenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen
- [EFS.5] EFS-Zugangspunkte sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden

- [ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden
- [ELB.2] Classic Load Balancer mit SSL/HTTPS-Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden
- [ELB.4] Application Load Balancer sollte so konfiguriert sein, dass HTTP-Header gelöscht werden
- [ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config
- [ELB.9] Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.16] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF
- [ElastiCache.1] Bei ElastiCache Redis-Clustern sollte das automatische Backup aktiviert sein
- [ElastiCache.6] ElastiCache Für Redis-Replikationsgruppen vor Version 6.0 sollte Redis AUTH verwendet werden
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [ES.1] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein
- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein
- [EventBridge.2] EventBridge Eventbusse sollten gekennzeichnet sein
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden

- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [Glue.1] AWS Glue Jobs sollten markiert werden
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen werden
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden
- [IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden
- [IoT.3] AWS IoT Core -Dimensionen sollten markiert werden
- [IoT.4] AWS IoT Core Autorisierer sollten markiert werden
- [IoT.5] AWS IoT Core Rollenaliase sollten markiert werden

- [IoT.6] AWS IoT Core Richtlinien sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben

- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein
- Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben
- Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch -Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.
- [RDS.5] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden
- [RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.16] RDS-DB-Cluster sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein

- [Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein
- [Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein
- [S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [SNS.1] SNS-Themen sollten im Ruhezustand wie folgt verschlüsselt werden AWS KMS
- [SNS.3] SNS-Themen sollten markiert werden
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben

- [Transfer.1] AWS Transfer Family -Workflows sollten mit Tags versehen werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein

Israel (Tel Aviv)

Die folgenden Steuerelemente werden in Israel (Tel Aviv) nicht unterstützt.

- [ACM.1] Importierte und von ACM ausgestellte Zertifikate sollten nach einem bestimmten Zeitraum erneuert werden
- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [ApiGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben
- [ApiGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.4] AWS AppSync GraphQL-APIs sollten markiert werden
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden
- [Athena.3] Athena-Arbeitsgruppen sollten markiert werden
- [Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben

- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.3] AWS Backup Tresore sollten markiert sein
- [Backup.4] AWS Backup Berichtspläne sollten markiert werden
- [Backup.5] AWS Backup Backup-Pläne sollten markiert werden
- [CloudFormation.2] CloudFormation Stapel sollten markiert werden
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild1.4] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben

- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [Detective.1] Verhaltensdiagramme von Detektiven sollten markiert werden
- [DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
- [DMS.2] DMS-Zertifikate sollten gekennzeichnet sein
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.3] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden

- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein
- [EC2.10] Amazon EC2 sollte so konfiguriert sein, dass es VPC-Endpunkte verwendet, die für den Amazon EC2-Service erstellt wurden
- [EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen
- [EC2.14] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulassen
- [EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen
- [EC2.20] Beide VPN-Tunnel für eine AWS Site-to-Site-VPN-Verbindung sollten aktiv sein
- [EC2.22] Ungenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.33] EC2 Transit Gateway-Anhänge sollten markiert werden
- [EC2.34] Die Routentabellen des EC2-Transit-Gateways sollten mit Tags versehen werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.48] Amazon VPC-Flow-Logs sollten markiert werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [EC2.52] EC2-Transit-Gateways sollten markiert werden
- [ECR.2] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS

- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen
- [EFS.5] EFS-Zugangspunkte sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [EKS.6] EKS-Cluster sollten markiert werden
- [EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden
- [EKS.8] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein
- [ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden
- [ELB.2] Classic Load Balancer mit SSL/HTTPS-Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.4] Application Load Balancer sollte so konfiguriert sein, dass HTTP-Header gelöscht werden
- [ELB.6] Für Anwendungen, Gateways und Network Load Balancers sollte der Löschschutz aktiviert sein
- [ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config
- [ELB.13] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.16] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF
- [ElastiCache.1] Bei ElastiCache Redis-Clustern sollte das automatische Backup aktiviert sein
- [ElastiCache.2] ElastiCache Für Redis-Cache-Cluster sollte das auto Upgrade der Nebenversion aktiviert sein
- [ElastiCache.3] ElastiCache Für Redis-Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache für Redis-Replikationsgruppen sollten im Ruhezustand verschlüsselt werden

- [ElastiCache.5] ElastiCache für Redis-Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache Für Redis-Replikationsgruppen vor Version 6.0 sollte Redis AUTH verwendet werden
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [ES.1] Bei Elasticsearch-Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein
- [ES.3] Elasticsearch-Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein
- [EventBridge.2] EventBridge Eventbusse sollten gekennzeichnet sein
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen werden
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein
- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden

- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen
- [IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.
- [IAM.7] Die Passwortrichtlinien für IAM-Benutzer sollten stark konfiguriert sein
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.10] Passwortrichtlinien für IAM-Benutzer sollten strenge Laufzeiten haben AWS Config
- [IAM.11] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Großbuchstaben erfordert
- [IAM.12] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens einen Kleinbuchstaben erfordert
- [IAM.13] Stellen Sie sicher, dass für die IAM-Passwortrichtlinie mindestens ein Symbol erforderlich ist
- [IAM.14] Stellen Sie sicher, dass die IAM-Passwortrichtlinie mindestens eine Zahl erfordert
- [IAM.15] Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestkennwortlänge von 14 oder mehr erfordert
- [IAM.16] Stellen Sie sicher, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert
- [IAM.17] Stellen Sie sicher, dass die IAM-Passwortrichtlinie Passwörter innerhalb von 90 Tagen oder weniger abläuft
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.23] IAM Access Analyzer-Analyzer sollten markiert werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess

- [IAM.28] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein
- [IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden
- [IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden
- [IoT.3] AWS IoT Core -Dimensionen sollten markiert werden
- [IoT.4] AWS IoT Core Autorisierer sollten markiert werden
- [IoT.5] AWS IoT Core Rollenaliase sollten markiert werden
- [IoT.6] AWS IoT Core Richtlinien sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [Kinesis.2] Kinesis-Streams sollten markiert werden
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Macie.1] Amazon Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren

- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein
- Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben
- Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch -Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [PCA.1] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein
- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.4] RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden
- [RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein

- [RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein
- [RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.16] RDS-DB-Cluster sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.28] RDS-DB-Cluster sollten markiert werden
- [RDS.29] RDS-DB-Cluster-Snapshots sollten mit Tags versehen werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein
- [Redshift.3] Bei Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein
- [Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden
- [Redshift.9] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden
- [Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein
- [S3.2] S3-Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren
- [S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren
- [S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren
- [S3.9] Bei S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben

- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SecretsManager.1] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein
- [SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren
- [SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen
- [SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [SNS.1] SNS-Themen sollten im Ruhezustand wie folgt verschlüsselt werden AWS KMS
- [SNS.3] SNS-Themen sollten markiert werden
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [SSM.3] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten den Zuordnungs-Compliance-Status COMPLIANT haben
- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [StepFunctions.2] Die Aktivitäten von Step Functions sollten markiert werden
- [Transfer.1] AWS Transfer Family -Workflows sollten mit Tags versehen werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden

- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein
- Für [WAF.12] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch

Naher Osten (Bahrain)

Die folgenden Steuerelemente werden im Nahen Osten (Bahrain) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden

- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.20] Beide VPN-Tunnel für eine AWS Site-to-Site-VPN-Verbindung sollten aktiv sein
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden

- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein
- [RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.16] RDS-DB-Cluster sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [Redshift.6] Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [SSM.2] Von Systems Manager verwaltete Amazon EC2 EC2-Instances sollten nach einer Patch-Installation den Patch-Compliance-Status COMPLIANT haben
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben

- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

Naher Osten (VAE)

Die folgenden Steuerelemente werden im Nahen Osten (VAE) nicht unterstützt.

- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [ApiGateway.1] API Gateway REST und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein
- [ApiGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben
- [ApiGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden
- [Athena.3] Athena-Arbeitsgruppen sollten markiert werden
- [AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden
- [Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.4] AWS Backup Berichtspläne sollten markiert werden
- [Backup.5] AWS Backup Backup-Pläne sollten markiert werden
- [CloudFormation.2] CloudFormation Stapel sollten markiert werden
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten

- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst
- [CloudTrail.6] Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist
- [CloudWatch.15] Für CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein
- [CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden
- [CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild1.4] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [Detective.1] Verhaltensdiagramme von Detektiven sollten markiert werden
- [DMS.1] Replikationsinstanzen des Database Migration Service sollten nicht öffentlich sein
- [DMS.2] DMS-Zertifikate sollten gekennzeichnet sein
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden

- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.3] Angehängte Amazon EBS-Volumes sollten im Ruhezustand verschlüsselt werden
- [EC2.4] Gestoppte EC2-Instances sollten nach einem bestimmten Zeitraum entfernt werden
- [EC2.6] Die VPC-Flow-Protokollierung sollte in allen VPCs aktiviert sein
- [EC2.8] EC2-Instances sollten Instance Metadata Service Version 2 (IMDSv2) verwenden
- [EC2.12] Ungenutzte Amazon EC2 EC2-EIPs sollten entfernt werden
- [EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen
- [EC2.14] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulassen
- [EC2.22] Ungenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden

- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [EFS.1] Elastic File System sollte so konfiguriert sein, dass ruhende Dateidaten verschlüsselt werden mit AWS KMS
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden
- [ELB.3] Classic Load Balancer Balancer-Listener sollten mit HTTPS- oder TLS-Terminierung konfiguriert werden
- [ELB.9] Bei Classic Load Balancers sollte der zonenübergreifende Load Balancing aktiviert sein
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.16] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF

- [ElastiCache.1] Bei ElastiCache Redis-Clustern sollte das automatische Backup aktiviert sein
- [ElastiCache.2] ElastiCache Für Redis-Cache-Cluster sollte das auto Upgrade der Nebenversion aktiviert sein
- [ElastiCache.3] ElastiCache Für Redis-Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache für Redis-Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache für Redis-Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache Für Redis-Replikationsgruppen vor Version 6.0 sollte Redis AUTH verwendet werden
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben
- [EventBridge.2] EventBridge Eventbusse sollten gekennzeichnet sein
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen werden
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [IAM.1] IAM-Richtlinien sollten keine vollen „*“ -Administratorrechte zulassen
- [IAM.2] IAM-Benutzern sollten keine IAM-Richtlinien zugeordnet sein

- [IAM.3] Die Zugriffsschlüssel von IAM-Benutzern sollten alle 90 Tage oder weniger gewechselt werden
- [IAM.4] Der IAM-Root-Benutzerzugriffsschlüssel sollte nicht existieren
- [IAM.5] MFA sollte für alle -Benutzer aktiviert sein, die über ein Konsolenpasswort verfügen
- [IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.
- [IAM.8] Unbenutzte IAM-Benutzeranmeldedaten sollten entfernt werden
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.18] Stellen Sie sicher, dass eine Support-Rolle für die Verwaltung von Vorfällen eingerichtet wurde AWS Support
- [IAM.19] MFA sollte für alle IAM-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.22] IAM-Benutzeranmeldedaten, die 45 Tage lang nicht verwendet wurden, sollten entfernt werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess
- [IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden
- [IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden
- [IoT.3] AWS IoT Core -Dimensionen sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [KMS.1] Kundenverwaltete IAM-Richtlinien sollten keine Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.2] IAM-Prinzipale sollten keine IAM-Inline-Richtlinien haben, die Entschlüsselungsaktionen für alle KMS-Schlüssel zulassen
- [KMS.4] Die AWS KMS Schlüsselrotation sollte aktiviert sein
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch

- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.7] Netzwerk-Firewall-Firewalls sollten markiert werden
- [NetworkFirewall.8] Firewall-Richtlinien für Netzwerk-Firewalls sollten markiert werden
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein

- Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben
- Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch -Domains sollten mit Tags versehen werden
- Auf [Opensearch.10] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.1] Der RDS-Snapshot sollte privat sein
- [RDS.2] RDS-DB-Instances sollten je nach Dauer den öffentlichen Zugriff verbieten PubliclyAccessible AWS Config
- [RDS.3] Für RDS-DB-Instances sollte die Verschlüsselung im Ruhezustand aktiviert sein.
- [RDS.5] RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden
- [RDS.6] Die erweiterte Überwachung sollte für RDS-DB-Instances konfiguriert werden
- [RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein
- [RDS.11] Bei RDS-Instances sollten automatische Backups aktiviert sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.16] RDS-DB-Cluster sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein
- [Redshift.9] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden
- [Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [S3.2] S3-Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren
- [S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren

- [S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern
- [S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten
- [S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SecretsManager.1] Bei Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein
- [SecretsManager.2] Secrets Manager Manager-Geheimnisse, die mit automatischer Rotation konfiguriert sind, sollten erfolgreich rotieren
- [SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen
- [SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [SNS.1] SNS-Themen sollten im Ruhezustand wie folgt verschlüsselt werden AWS KMS
- [SNS.3] SNS-Themen sollten markiert werden
- [SQS.1] Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SSM.1] Amazon EC2 EC2-Instances sollten verwaltet werden von AWS Systems Manager
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [Transfer.1] AWS Transfer Family -Workflows sollten mit Tags versehen werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein

- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein

Südamerika (São Paulo)

Die folgenden Steuerelemente werden in Südamerika (São Paulo) nicht unterstützt.

- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden

- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden
- [IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden
- [IoT.3] AWS IoT Core -Dimensionen sollten markiert werden
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein
- [RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.16] RDS-DB-Cluster sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen

- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

AWS GovCloud (US-Ost)

Die folgenden Steuerelemente werden in AWS GovCloud (USA-Ost) nicht unterstützt.

- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [ACM.3] ACM-Zertifikate sollten mit einem Tag versehen werden
- [Account.1] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto
- [Account.2] AWS-Konten sollte Teil einer Organisation sein AWS Organizations
- [ApiGateway.2] API Gateway REST-API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [ApiGateway.3] Bei den REST-API-Stufen von API Gateway sollte die Ablaufverfolgung aktiviert sein AWS X-Ray
- [ApiGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein
- [ApiGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben
- [ApiGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.4] AWS AppSync GraphQL-APIs sollten markiert werden

- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden
- [Athena.3] Athena-Arbeitsgruppen sollten markiert werden
- [AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken
- [AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen
- [AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden
- [AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden
- [AutoScaling.10] EC2 Auto Scaling Scaling-Gruppen sollten markiert werden
- [Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.3] AWS Backup Tresore sollten markiert sein
- [Backup.4] AWS Backup Berichtspläne sollten markiert werden
- [Backup.5] AWS Backup Backup-Pläne sollten markiert werden
- [CloudFormation.2] CloudFormation Stapel sollten markiert werden
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden

- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen
- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CloudTrail.9] CloudTrail Pfade sollten markiert werden
- [CloudWatch.15] Für CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein
- [CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden
- [CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild1.4] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [Detective.1] Verhaltensdiagramme von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten gekennzeichnet sein
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein

- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein
- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.1] DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.5] DynamoDB-Tabellen sollten mit Tags versehen werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen
- [EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden
- [EC2.17] Amazon EC2 EC2-Instances sollten nicht mehrere ENIs verwenden
- [EC2.21] Netzwerk-ACLs sollten keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen
- [EC2.22] Ungenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.33] EC2 Transit Gateway-Anhänge sollten markiert werden
- [EC2.34] Die Routentabellen des EC2-Transit-Gateways sollten mit Tags versehen werden
- [EC2.35] EC2-Netzwerkschnittstellen sollten markiert werden
- [EC2.36] EC2-Kunden-Gateways sollten mit Tags versehen werden

- [EC2.37] EC2-Elastic-IP-Adressen sollten mit Tags versehen werden
- [EC2.38] EC2-Instances sollten markiert werden
- [EC2.39] EC2-Internet-Gateways sollten markiert werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.41] EC2-Netzwerk-ACLs sollten markiert werden
- [EC2.42] EC2-Routing-Tabellen sollten mit Tags versehen werden
- [EC2.43] EC2-Sicherheitsgruppen sollten markiert werden
- [EC2.44] EC2-Subnetze sollten markiert werden
- [EC2.45] EC2-Volumes sollten markiert werden
- [EC2.46] Amazon VPCs sollten markiert werden
- [EC2.47] Amazon VPC Endpoint Services sollten markiert werden
- [EC2.48] Amazon VPC-Flow-Logs sollten markiert werden
- [EC2.49] Amazon VPC-Peering-Verbindungen sollten markiert werden
- [EC2.50] EC2-VPN-Gateways sollten markiert werden
- [EC2.52] EC2-Transit-Gateways sollten markiert werden
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.
- [ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen
- [ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden
- [ECS.5] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein
- [ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [ECS.10] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen
- [ECS.12] ECS-Cluster sollten Container Insights verwenden
- [ECS.13] ECS-Services sollten markiert werden

- [ECS.14] ECS-Cluster sollten markiert werden
- [ECS.15] ECS-Aufgabendefinitionen sollten mit Tags versehen werden
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen
- [EFS.5] EFS-Zugangspunkte sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [EKS.6] EKS-Cluster sollten markiert werden
- [EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden
- [EKS.8] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein
- [ELB.2] Classic Load Balancer mit SSL/HTTPS-Listenern sollten ein Zertifikat verwenden, das bereitgestellt wird von AWS Certificate Manager
- [ELB.8] Classic Load Balancer mit SSL-Listenern sollten eine vordefinierte Sicherheitsrichtlinie mit starker Dauer verwenden AWS Config
- [ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken
- [ELB.12] Application Load Balancer sollte mit dem defensiven Modus oder dem strengsten Modus zur Desynchronisierung konfiguriert werden
- [ELB.13] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.16] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF
- [ElastiCache.1] Bei ElastiCache Redis-Clustern sollte das automatische Backup aktiviert sein
- [ElastiCache.2] ElastiCache Für Redis-Cache-Cluster sollte das auto Upgrade der Nebenversion aktiviert sein
- [ElastiCache.3] ElastiCache Für Redis-Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache für Redis-Replikationsgruppen sollten im Ruhezustand verschlüsselt werden

- [ElastiCache.5] ElastiCache für Redis-Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache Für Redis-Replikationsgruppen vor Version 6.0 sollte Redis AUTH verwendet werden
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden
- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.2] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein
- [ES.9] Elasticsearch-Domains sollten markiert werden
- [EventBridge.2] EventBridge Eventbusse sollten gekennzeichnet sein
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [Glue.1] AWS Glue Jobs sollten markiert werden
- [GuardDuty.1] GuardDuty sollte aktiviert sein
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen werden
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.23] IAM Access Analyzer-Analyzer sollten markiert werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden

- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden
- [IAM.28] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein
- [IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden
- [IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden
- [IoT.3] AWS IoT Core -Dimensionen sollten markiert werden
- [IoT.4] AWS IoT Core Autorisierer sollten markiert werden
- [IoT.5] AWS IoT Core Rollenaliase sollten markiert werden
- [IoT.6] AWS IoT Core Richtlinien sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [Kinesis.2] Kinesis-Streams sollten markiert werden
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Lambda.6] Lambda-Funktionen sollten markiert werden
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren

- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben
- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.7] Netzwerk-Firewall-Firewalls sollten markiert werden
- [NetworkFirewall.8] Firewall-Richtlinien für Netzwerk-Firewalls sollten markiert werden
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein
- Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben
- Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch -Domains sollten mit Tags versehen werden
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [PCA.1] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein
- [RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden
- [RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein

- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden
- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.28] RDS-DB-Cluster sollten markiert werden
- [RDS.29] RDS-DB-Cluster-Snapshots sollten mit Tags versehen werden
- [RDS.30] RDS-DB-Instances sollten markiert werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.32] RDS-DB-Snapshots sollten markiert werden
- [RDS.33] RDS-DB-Subnetzgruppen sollten markiert werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein
- [Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden
- [Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden
- [Redshift.9] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.11] Redshift-Cluster sollten markiert werden
- [Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden
- [Redshift.13] Redshift-Cluster-Snapshots sollten markiert werden
- [Redshift.14] Redshift-Cluster-Subnetzgruppen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein
- [S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren

- [S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben
- [S3.11] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein
- [S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten
- [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben
- [S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein
- [S3.20] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein
- [SageMaker.1] SageMaker Amazon-Notebook-Instances sollten keinen direkten Internetzugang haben
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen
- [SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden
- [SecretsManager.5] Secrets Manager Manager-Geheimnisse sollten markiert werden
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [SNS.3] SNS-Themen sollten markiert werden
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [StepFunctions.2] Die Aktivitäten von Step Functions sollten markiert werden
- [Transfer.1] AWS Transfer Family -Workflows sollten mit Tags versehen werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein

- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein
- Für [WAF.12] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch

AWS GovCloud (US-West)

Die folgenden Steuerelemente werden in AWS GovCloud (US-West) nicht unterstützt.

- [ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden
- [ACM.3] ACM-Zertifikate sollten mit einem Tag versehen werden
- [Account.1] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto
- [Account.2] AWS-Konten sollte Teil einer Organisation sein AWS Organizations
- [ApiGateway.2] API Gateway REST-API-Stufen sollten so konfiguriert werden, dass sie SSL-Zertifikate für die Backend-Authentifizierung verwenden
- [ApiGateway.3] Bei den REST-API-Stufen von API Gateway sollte die Ablaufverfolgung aktiviert sein AWS X-Ray
- [ApiGateway.4] API Gateway sollte mit einer WAF-Web-ACL verknüpft sein
- [ApiGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben
- [ApiGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein
- [AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben
- [AppSync.4] AWS AppSync GraphQL-APIs sollten markiert werden
- [AppSync.5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden
- [Athena.2] Athena-Datenkataloge sollten mit Tags versehen werden

- [Athena.3] Athena-Arbeitsgruppen sollten markiert werden
- [AutoScaling.2] Die Amazon EC2 Auto Scaling Scaling-Gruppe sollte mehrere Availability Zones abdecken
- [AutoScaling.3] Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2-Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen
- [AutoScaling.6] Auto Scaling Scaling-Gruppen sollten mehrere Instance-Typen in mehreren Availability Zones verwenden
- [AutoScaling.9] Amazon EC2 Auto Scaling Scaling-Gruppen sollten Amazon EC2 EC2-Startvorlagen verwenden
- [AutoScaling.10] EC2 Auto Scaling Scaling-Gruppen sollten markiert werden
- [Autoscaling.5] Amazon EC2 EC2-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben
- [Backup.2] AWS Backup Wiederherstellungspunkte sollten markiert werden
- [Backup.3] AWS Backup Tresore sollten markiert sein
- [Backup.4] AWS Backup Berichtspläne sollten markiert werden
- [Backup.5] AWS Backup Backup-Pläne sollten markiert werden
- [CloudFormation.2] CloudFormation Stapel sollten markiert werden
- Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein
- [CloudFront.3] CloudFront Distributionen sollten während der Übertragung verschlüsselt werden müssen
- [CloudFront.4] Bei CloudFront Distributionen sollte das Origin-Failover konfiguriert sein
- [CloudFront.5] Bei CloudFront Distributionen sollte die Protokollierung aktiviert sein
- [CloudFront.6] Bei CloudFront Distributionen sollte WAF aktiviert sein
- [CloudFront.7] CloudFront Distributionen sollten benutzerdefinierte SSL/TLS-Zertifikate verwenden
- [CloudFront.8] CloudFront Distributionen sollten SNI verwenden, um HTTPS-Anfragen zu bearbeiten
- [CloudFront.9] CloudFront Distributionen sollten den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln
- [CloudFront.10] CloudFront Distributionen sollten keine veralteten SSL-Protokolle zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden
- [CloudFront.12] CloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen

- [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden
- [CloudFront.14] CloudFront Distributionen sollten mit Tags versehen werden
- [CloudTrail.9] CloudTrail Pfade sollten markiert werden
- [CloudWatch.15] Für CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein
- [CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden
- [CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein
- [CodeArtifact.1] CodeArtifact Repositorien sollten mit Tags versehen werden
- [CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten
- [CodeBuild.2] CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten
- [CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein
- [CodeBuild1.4] CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben
- [DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden
- [Detective.1] Verhaltensdiagramme von Detektiven sollten markiert werden
- [DMS.2] DMS-Zertifikate sollten gekennzeichnet sein
- [DMS.3] DMS-Veranstaltungsabonnements sollten mit einem Tag versehen werden
- [DMS.4] DMS-Replikationsinstanzen sollten markiert werden
- [DMS.5] Subnetzgruppen für die DMS-Replikation sollten markiert werden
- [DMS.6] Für DMS-Replikationsinstanzen sollte das automatische Upgrade der Nebenversionen aktiviert sein
- [DMS.7] Bei DMS-Replikationsaufgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein
- [DMS.8] Bei DMS-Replikationsaufgaben für die Quelldatenbank sollte die Protokollierung aktiviert sein
- [DMS.9] DMS-Endpunkte sollten SSL verwenden
- [DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein
- [DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein

- [DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein
- [DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden
- [DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen
- [DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein
- [DocumentDB.4] Amazon DocumentDB-Cluster sollten Auditprotokolle in Logs veröffentlichen CloudWatch
- [DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein
- [DynamoDB.1] DynamoDB-Tabellen sollten die Kapazität automatisch bei Bedarf skalieren
- [DynamoDB.3] DynamoDB Accelerator (DAX) -Cluster sollten im Ruhezustand verschlüsselt werden
- [DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein
- [DynamoDB.5] DynamoDB-Tabellen sollten mit Tags versehen werden
- [DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden
- [EC2.15] Amazon EC2-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen
- [EC2.16] Unbenutzte Network Access Control Lists sollten entfernt werden
- [EC2.17] Amazon EC2 EC2-Instances sollten nicht mehrere ENIs verwenden
- [EC2.21] Netzwerk-ACLs sollten keinen Zugang von 0.0.0.0/0 zu Port 22 oder Port 3389 zulassen
- [EC2.22] Ungenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden
- [EC2.23] Amazon EC2 Transit Gateways sollten VPC-Anhangsanfragen nicht automatisch akzeptieren
- [EC2.24] Paravirtuelle Amazon EC2 EC2-Instance-Typen sollten nicht verwendet werden
- [EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen
- [EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden
- [EC2.33] EC2 Transit Gateway-Anhänge sollten markiert werden
- [EC2.34] Die Routentabellen des EC2-Transit-Gateways sollten mit Tags versehen werden
- [EC2.35] EC2-Netzwerkschnittstellen sollten markiert werden
- [EC2.36] EC2-Kunden-Gateways sollten mit Tags versehen werden
- [EC2.37] EC2-Elastic-IP-Adressen sollten mit Tags versehen werden

- [EC2.38] EC2-Instances sollten markiert werden
- [EC2.39] EC2-Internet-Gateways sollten markiert werden
- [EC2.40] EC2-NAT-Gateways sollten markiert werden
- [EC2.41] EC2-Netzwerk-ACLs sollten markiert werden
- [EC2.42] EC2-Routing-Tabellen sollten mit Tags versehen werden
- [EC2.43] EC2-Sicherheitsgruppen sollten markiert werden
- [EC2.44] EC2-Subnetze sollten markiert werden
- [EC2.45] EC2-Volumes sollten markiert werden
- [EC2.46] Amazon VPCs sollten markiert werden
- [EC2.47] Amazon VPC Endpoint Services sollten markiert werden
- [EC2.48] Amazon VPC-Flow-Logs sollten markiert werden
- [EC2.49] Amazon VPC-Peering-Verbindungen sollten markiert werden
- [EC2.50] EC2-VPN-Gateways sollten markiert werden
- [EC2.52] EC2-Transit-Gateways sollten markiert werden
- [ECR.1] Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein
- [ECR.2] Bei privaten ECR-Repositorys sollte die Tag-Unveränderlichkeit konfiguriert sein
- [ECR.3] Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein
- [ECR.4] Öffentliche ECR-Repositorien sollten markiert werden
- [ECS.1] Amazon ECS-Aufgabendefinitionen sollten sichere Netzwerkmodi und Benutzerdefinitionen enthalten.
- [ECS.3] ECS-Aufgabendefinitionen sollten den Prozess-Namespace des Hosts nicht gemeinsam nutzen
- [ECS.4] ECS-Container sollten ohne Zugriffsrechte ausgeführt werden
- [ECS.5] ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein
- [ECS.8] Geheimnisse sollten nicht als Container-Umgebungsvariablen übergeben werden
- [ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen
- [ECS.10] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen
- [ECS.12] ECS-Cluster sollten Container Insights verwenden
- [ECS.13] ECS-Services sollten markiert werden
- [ECS.14] ECS-Cluster sollten markiert werden

- [ECS.15] ECS-Aufgabendefinitionen sollten mit Tags versehen werden
- [EFS.2] Amazon EFS-Volumes sollten in Backup-Plänen enthalten sein
- [EFS.3] EFS-Zugriffspunkte sollten ein Stammverzeichnis erzwingen
- [EFS.4] EFS-Zugangspunkte sollten eine Benutzeridentität erzwingen
- [EFS.5] EFS-Zugangspunkte sollten markiert werden
- [EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden
- [EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein
- [EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden
- [EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden
- [EKS.6] EKS-Cluster sollten markiert werden
- [EKS.7] Die Konfigurationen des EKS-Identitätsanbieters sollten mit Tags versehen werden
- [EKS.8] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein
- [ELB.10] Classic Load Balancer sollte sich über mehrere Availability Zones erstrecken
- [ELB.12] Application Load Balancer sollte mit dem defensiven Modus oder dem strengsten Modus zur Desynchronisierung konfiguriert werden
- [ELB.13] Anwendungs-, Netzwerk- und Gateway-Load Balancer sollten sich über mehrere Availability Zones erstrecken
- [ELB.14] Classic Load Balancer sollte mit einem defensiven oder strengsten Desync-Minimationsmodus konfiguriert werden
- [ELB.16] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF
- [ElastiCache.1] Bei ElastiCache Redis-Clustern sollte das automatische Backup aktiviert sein
- [ElastiCache.2] ElastiCache Für Redis-Cache-Cluster sollte das auto Upgrade der Nebenversion aktiviert sein
- [ElastiCache.3] ElastiCache Für Redis-Replikationsgruppen sollte der automatische Failover aktiviert sein
- [ElastiCache.4] ElastiCache für Redis-Replikationsgruppen sollten im Ruhezustand verschlüsselt werden
- [ElastiCache.5] ElastiCache für Redis-Replikationsgruppen sollten bei der Übertragung verschlüsselt werden
- [ElastiCache.6] ElastiCache Für Redis-Replikationsgruppen vor Version 6.0 sollte Redis AUTH verwendet werden
- [ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden

- [ElasticBeanstalk.1] Elastic Beanstalk Beanstalk-Umgebungen sollten erweiterte Gesundheitsberichte aktiviert haben
- [ElasticBeanstalk.2] Von Elastic Beanstalk verwaltete Plattformupdates sollten aktiviert sein
- [ElasticBeanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch
- [EMR.2] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein
- [ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein
- [ES.9] Elasticsearch-Domains sollten markiert werden
- [EventBridge.2] EventBridge Eventbusse sollten gekennzeichnet sein
- [EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden
- [EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein
- [FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden
- [FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden
- [GlobalAccelerator.1] Global Accelerator-Beschleuniger sollten gekennzeichnet sein
- [Glue.1] AWS Glue Jobs sollten markiert werden
- [GuardDuty.2] GuardDuty Filter sollten mit Tags versehen werden
- [GuardDuty.3] GuardDuty IPSets sollten markiert werden
- [GuardDuty.4] GuardDuty Detektoren sollten markiert werden
- [IAM.6] Hardware-MFA sollte für den Stammbenutzer aktiviert sein.
- [IAM.9] MFA sollte für den Root-Benutzer aktiviert sein
- [IAM.21] Kundenverwaltete IAM-Richtlinien, die Sie erstellen, sollten keine Platzhalteraktionen für Dienste zulassen
- [IAM.23] IAM Access Analyzer-Analyzer sollten markiert werden
- [IAM.24] IAM-Rollen sollten mit Tags versehen werden
- [IAM.25] IAM-Benutzer sollten markiert werden
- [IAM.28] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein
- [IoT.1] AWS IoT Core Sicherheitsprofile sollten markiert werden
- [IoT.2] AWS IoT Core Minderungsmaßnahmen sollten gekennzeichnet werden
- [IoT.3] AWS IoT Core -Dimensionen sollten markiert werden

- [IoT.4] AWS IoT Core Autorisierer sollten markiert werden
- [IoT.5] AWS IoT Core Rollenaliase sollten markiert werden
- [IoT.6] AWS IoT Core Richtlinien sollten markiert werden
- [Kinesis.1] Kinesis-Streams sollten im Ruhezustand verschlüsselt werden
- [Kinesis.2] Kinesis-Streams sollten markiert werden
- [Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren
- [Lambda.6] Lambda-Funktionen sollten markiert werden
- [Macie.1] Amazon Macie sollte aktiviert sein
- [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein
- [MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch
- [MQ.3] Bei Amazon MQ-Brokern sollte das automatische Upgrade der Nebenversion aktiviert sein
- [MQ.4] Amazon MQ-Broker sollten markiert werden
- [MQ.5] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden
- [MQ.6] RabbitMQ-Broker sollten den Cluster-Bereitstellungsmodus verwenden
- [MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden
- [MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein
- [Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein
- [Neptune.4] Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein
- [Neptune.5] Bei Neptune-DB-Clustern sollten automatische Backups aktiviert sein
- [Neptune.6] Neptune-DB-Cluster-Snapshots sollten im Ruhezustand verschlüsselt werden
- [Neptune.7] Bei Neptune-DB-Clustern sollte die IAM-Datenbankauthentifizierung aktiviert sein
- [Neptune.8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren
- [Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden
- [NetworkFirewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden
- [NetworkFirewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein
- [NetworkFirewall.3] Netzwerk-Firewall-Richtlinien sollten mindestens eine Regelgruppe zugeordnet haben

- [NetworkFirewall.4] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für vollständige Pakete „Verwerfen“ oder „Weiterleiten“ sein.
- [NetworkFirewall.5] Die standardmäßige statuslose Aktion für Netzwerk-Firewall-Richtlinien sollte für fragmentierte Pakete „Drop“ oder „Forward“ sein.
- [NetworkFirewall.6] Die Regelgruppe Stateless Network Firewall sollte nicht leer sein
- [NetworkFirewall.7] Netzwerk-Firewall-Firewalls sollten markiert werden
- [NetworkFirewall.8] Firewall-Richtlinien für Netzwerk-Firewalls sollten markiert werden
- [NetworkFirewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein
- Bei [Opensearch.1] OpenSearch -Domains sollte die Verschlüsselung im Ruhezustand aktiviert sein
- [Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein
- [Opensearch.3] OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden
- Die Protokollierung von [Opensearch.4] OpenSearch Domain-Fehlern in CloudWatch Logs sollte aktiviert sein
- Für [Opensearch.5] OpenSearch -Domains sollte die Audit-Protokollierung aktiviert sein
- [Opensearch.6] OpenSearch -Domains sollten mindestens drei Datenknoten haben
- Für [Opensearch.7] OpenSearch -Domains sollte eine differenzierte Zugriffskontrolle aktiviert sein
- [Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden
- [Opensearch.9] OpenSearch -Domains sollten mit Tags versehen werden
- [Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben
- [PCA.1] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein
- [RDS.12] Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden
- [RDS.13] Automatische RDS-Upgrades für Nebenversionen sollten aktiviert sein
- [RDS.14] Bei Amazon Aurora Aurora-Clustern sollte Backtracking aktiviert sein
- [RDS.15] RDS-DB-Cluster sollten für mehrere Availability Zones konfiguriert werden
- [RDS.24] RDS-Datenbankcluster sollten einen benutzerdefinierten Administratorbenutzernamen verwenden
- [RDS.25] RDS-Datenbank-Instances sollten einen benutzerdefinierten Administrator-Benutzernamen verwenden
- [RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden

- [RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden
- [RDS.28] RDS-DB-Cluster sollten markiert werden
- [RDS.29] RDS-DB-Cluster-Snapshots sollten mit Tags versehen werden
- [RDS.30] RDS-DB-Instances sollten markiert werden
- [RDS.31] RDS-DB-Sicherheitsgruppen sollten markiert werden
- [RDS.32] RDS-DB-Snapshots sollten markiert werden
- [RDS.33] RDS-DB-Subnetzgruppen sollten markiert werden
- [RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch
- [RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein
- [Redshift.7] Redshift-Cluster sollten erweitertes VPC-Routing verwenden
- [Redshift.8] Amazon Redshift Redshift-Cluster sollten nicht den standardmäßigen Admin-Benutzernamen verwenden
- [Redshift.9] Redshift-Cluster sollten nicht den Standard-Datenbanknamen verwenden
- [Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden
- [Redshift.11] Redshift-Cluster sollten markiert werden
- [Redshift.12] Abonnements für Redshift-Ereignisbenachrichtigungen sollten markiert werden
- [Redshift.13] Redshift-Cluster-Snapshots sollten markiert werden
- [Redshift.14] Redshift-Cluster-Subnetzgruppen sollten markiert werden
- [Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen
- [Route 53.1] Route 53-Zustandsprüfungen sollten gekennzeichnet sein
- [Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren
- [S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein
- [S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren
- [S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben
- [S3.11] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein
- [S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten
- [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben
- [S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein

- [S3.20] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein
- [SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden
- [SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben
- [SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein
- [SES.1] SES-Kontaktlisten sollten mit Tags versehen werden
- [SES.2] SES-Konfigurationssätze sollten mit Tags versehen werden
- [SecretsManager.3] Unbenutzte Secrets Manager Manager-Geheimnisse entfernen
- [SecretsManager.4] Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden
- [SecretsManager.5] Secrets Manager Manager-Geheimnisse sollten markiert werden
- [ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS Organisation gemeinsam genutzt werden
- [SNS.3] SNS-Themen sollten markiert werden
- [SQS.2] SQS-Warteschlangen sollten markiert werden
- [SSM.4] SSM-Dokumente sollten nicht öffentlich sein
- [StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben
- [StepFunctions.2] Die Aktivitäten von Step Functions sollten markiert werden
- [Transfer.1] AWS Transfer Family -Workflows sollten mit Tags versehen werden
- [Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden
- [WAF.1] Die AWS WAF klassische globale Web-ACL-Protokollierung sollte aktiviert sein
- [WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben
- [WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben
- [WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben
- [WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben
- [WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben

- [WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben
- [WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein
- Für [WAF.12] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch

Security Hub deaktivieren

> **Note**
>
> Wenn Sie die zentrale Konfiguration verwenden, kann der delegierte AWS Security Hub-Administrator Konfigurationsrichtlinien erstellen, die Security Hub in bestimmten Konten und Organisationseinheiten (OUs) deaktivieren und in anderen aktivieren. Die Konfigurationsrichtlinien gelten in Ihrer Heimatregion und allen verknüpften Regionen. Weitere Informationen finden Sie unter So funktioniert die zentrale Konfiguration.

Sie können die Security Hub-Konsole, die Security Hub Hub-API oder AWS CLI zum Deaktivieren von Security Hub verwenden.

Folgendes passiert, wenn Sie Security Hub für ein Konto deaktivieren:

- Für das Konto werden keine neuen Erkenntnisse verarbeitet.
- Nach 90 Tagen werden Ihre vorhandenen Ergebnisse und Erkenntnisse sowie alle Security Hub Hub-Konfigurationseinstellungen gelöscht und können nicht wiederhergestellt werden.

  Wenn Sie Ihre vorhandenen Ergebnisse speichern möchten, müssen Sie sie exportieren, bevor Sie Security Hub deaktivieren. Weitere Informationen finden Sie unter the section called “Auswirkung von Kontoaktionen auf Security Hub Hub-Daten”.
- Alle aktivierten Standards und Kontrollen sind deaktiviert.

In den folgenden Fällen können Sie Security Hub nicht deaktivieren:

- Ihr Konto ist das designierte Security Hub-Administratorkonto für eine Organisation. Wenn Sie die zentrale Konfiguration verwenden, können Sie dem delegierten Administratorkonto keine Konfigurationsrichtlinie zuordnen, die Security Hub deaktiviert. Die Zuordnung kann für andere Konten erfolgreich sein, aber Security Hub wendet eine solche Richtlinie nicht auf das delegierte Administratorkonto an.
- Ihr Konto ist auf Einladung ein Security Hub-Administratorkonto, und Sie haben Mitgliedskonten, die aktiviert sind. Bevor Sie Security Hub deaktivieren können, müssen Sie alle Ihre Mitgliedskonten trennen. Siehe the section called “Aufheben der Zuordnung von Mitgliedskonten”.

Bevor Sie Security Hub für ein Mitgliedskonto deaktivieren können, muss das Konto von seinem Administratorkonto getrennt werden. Bei einem Organisationskonto kann nur das Administratorkonto die Zuordnung von Mitgliedskonten trennen. Weitere Informationen finden Sie unter the section called “Aufheben der Zuordnung von Mitgliedskonten der Organisation”. Bei manuell eingeladenen Konten kann entweder das Administratorkonto oder das Mitgliedskonto die Verknüpfung des Mitgliedskontos aufheben. Weitere Informationen finden Sie unter the section called “Aufheben der Zuordnung von Mitgliedskonten” oder the section called “Trennen der Verbindung zu Ihrem Administratorkonto”. Eine Trennung der Verbindung ist nicht erforderlich, wenn Sie die zentrale Konfiguration verwenden, da Sie eine Richtlinie erstellen können, die Security Hub in bestimmten Mitgliedskonten deaktiviert.

Wenn Sie Security Hub in einem Konto deaktivieren, ist es nur in der aktuellen Region deaktiviert. Wenn Sie jedoch die zentrale Konfiguration verwenden, um Security Hub in bestimmten Konten zu deaktivieren, ist es in der Heimatregion und allen verknüpften Regionen deaktiviert.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zur Deaktivierung von Security Hub.

Security Hub console

Um Security Hub zu deaktivieren

1. Öffnen Sie die AWS Security Hub Hub-Konsole unter https://console.aws.amazon.com/securityhub/.
2. Wählen Sie im Navigationsbereich Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Option Allgemein aus.
4. Wählen Sie unter AWS Security Hub deaktivieren die Option AWSSecurity Hub deaktivieren aus. Wählen Sie dann erneut Disable AWS Security Hub.

Security Hub API

Um Security Hub zu deaktivieren

Rufen Sie die `DisableSecurityHub`API auf.

AWS CLI

Um Security Hub zu deaktivieren

Führen Sie den Befehl `disable-security-hub` aus.

Beispielbefehl:

```
aws securityhub disable-security-hub
```

Änderungsprotokoll für Security Hub-Steuerelemente

Im folgenden Änderungsprotokoll werden wesentliche Änderungen an bestehenden AWS Security Hub Sicherheitskontrollen aufgezeichnet, die zu Änderungen des Gesamtstatus einer Kontrolle und des Compliance-Status der Ergebnisse führen können. Informationen darüber, wie Security Hub den Kontrollstatus auswertet, finden Sie unterKonformitätsstatus und Kontrollstatus. Es kann einige Tage nach ihrem Eintrag in diesem Protokoll dauern, bis sich Änderungen auf alle AWS-Regionen auswirken, für die das Steuerelement verfügbar ist.

In diesem Protokoll werden Änderungen aufgezeichnet, die seit April 2023 vorgenommen wurden.

Wählen Sie ein Steuerelement aus, um weitere Details dazu anzuzeigen. Titeländerungen werden 90 Tage lang in der detaillierten Beschreibung der einzelnen Kontrollen vermerkt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
8. Mai 2024	[S3.20] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein	Dieses Steuerelement prüft, ob bei einem versionsbasierten Amazon S3-Bucket für allgemeine Zwecke das Löschen mit Multi-Faktor-Authentifizierung (MFA) aktiviert ist. Zuvor ergab die Kontrolle einen `FAILED` Befund für Buckets, die über eine Lifecycle-Konfiguration verfügen. Das Löschen von MFA mit Versionierung kann jedoch nicht für einen Bucket aktiviert werden, der

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		über eine Lifecycle-Konfiguration verfügt. Security Hub hat das Steuerelement aktualisiert, sodass es keine Ergebnisse für Buckets mit einer Lifecycle-Konfiguration gibt. Die Beschreibung des Steuerelements wurde aktualisiert, um das aktuelle Verhalten widerzuspiegeln.
2. Mai 2024	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Security Hub hat die älteste unterstützte Version von Kubernetes, auf der der Amazon EKS-Cluster ausgeführt werden kann, aktualisiert, um ein bestehendes Ergebnis zu erzielen. Die derzeit älteste unterstützte Version ist Kubernetes. `1.26`

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
30. April 2024	[CloudTrail.3] Mindestens ein CloudTrail Trail sollte aktiviert sein	Der Titel des Steuerelements wurde von „CloudTrail sollte aktiviert“ auf „Mindestens ein CloudTrail Trail sollte aktiviert sein“ geändert. Dieses Steuerelement zeigt derzeit `PASSED` an AWS-Konto , ob für mindestens ein CloudTrail Trail aktiviert ist. Der Titel und die Beschreibung wurden geändert, um das aktuelle Verhalten genau widerzuspiegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
29. April 2024	[AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten ELB-Zustandsprüfungen verwenden	Der Titel der Steuerung wurde von Auto Scaling Scaling-Gruppen, die einem Classic Load Balancer zugeordnet sind, sollten Load Balancer-Integritätsprüfungen verwenden, zu Auto Scaling Scaling-G ruppen, die einem Load Balancer zugeordnet sind, ELB-Zustandsprüfun gen verwenden. Dieses Steuerele ment bewertet derzeit Anwendungs-, Gateway-, Netzwerk- und Classic Load Balancer. Der Titel und die Beschreibung wurden geändert, um das aktuelle Verhalten genau widerzusp iegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
19. April 2024	[CloudTrail.1] CloudTrail sollte aktiviert und mit mindestens einem regionsübergreifenden Trail konfiguriert sein, der Verwaltungsereignisse für Lese- und Schreibvorgänge umfasst	Das Steuerelement überprüft, ob AWS CloudTrail es aktiviert und mit mindesten s einem Multiregi onspfad konfiguriert ist, der Verwaltun gsereignisse für Lese- und Schreibvo rgänge umfasst. Bisher generierte das Steuerelement fälschlicherweise `PASSED` Ergebnisse, wenn ein Konto mit mindestens einem Multiregions-Trail CloudTrail aktiviert und konfiguriert war, auch wenn kein Trail Lese- und Schreibverwaltungs ereignisse aufzeichn ete. Das Steuerele ment generiert jetzt nur noch `PASSED` Ergebnisse, wenn CloudTrail es aktiviert und mit mindesten s einem multiregi onalen Trail konfiguri ert ist, der Verwaltun gsereignisse für Lese-

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		und Schreibvorgänge erfasst.
10. April 2024	[Athena.1] Athena-Arbeitsgruppen sollten im Ruhezustand verschlüsselt werden	Security Hub hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Athena-Arbeitsgruppen senden Protokolle an Amazon Simple Storage Service (Amazon S3) -Buckets. Amazon S3 bietet jetzt Standardverschlüsselung mit verwalteten S3-Schlüsseln (SS3-S3) für neue und bestehende S3-Buckets.
10. April 2024	[AutoScaling.4] Die Auto Scaling Scaling-Gruppenstartkonfiguration sollte kein Metadaten-Response-Hop-Limit größer als 1 haben	Security Hub hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Die Limits für Metadaten-Antwort-Hops für Amazon Elastic Compute Cloud (Amazon EC2) -Instances hängen von der Arbeitslast ab.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. April 2024	[CloudFormation.1] CloudFormation Stacks sollten in Simple Notification Service (SNS) integriert werden	Security Hub hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Die Integration von AWS CloudFormation Stacks mit Amazon SNS SNS-Themen ist keine bewährte Sicherheitsmethode mehr. Die Integration wichtiger CloudFormation Stacks mit SNS-Themen kann zwar nützlich sein, ist aber nicht für alle Stacks erforderlich.
10. April 2024	[CodeBuild.5] In CodeBuild Projektumgebungen sollte der privilegierte Modus nicht aktiviert sein	Security Hub hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Die Aktivierung des privilegierten Modus in einem CodeBuild Projekt stellt kein zusätzliches Risiko für die Kundenumgebung dar.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. April 2024	[IAM.20] Vermeiden Sie die Verwendung des Root-Benutzers	Security Hub hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Der Zweck dieser Kontrolle wird durch eine andere Kontrolle abgedeckt ,[CloudWatch.1] Für den Benutzer „root“ sollten ein Metrik-Logfilter und ein Alarm vorhanden sein.
10. April 2024	[SNS.2] Die Protokollierung des Zustellungsstatus sollte für Benachrichtigungen aktiviert werden, die an ein Thema gesendet werden	Security Hub hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Das Protokollieren des Zustellungsstatus für SNS-Themen ist keine bewährte Sicherheitsmethode mehr. Die Protokollierung des Zustellungsstatus für wichtige SNS-Themen kann zwar nützlich sein, ist aber nicht für alle Themen erforderlich.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. April 2024	[S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben	Security Hub hat dieses Steuerelement aus AWS Foundational Security Best Practices und Service-Managed Standard entfernt: . AWS Control Tower Der Zweck dieser Kontrolle wird durch zwei weitere Steuerelemente abgedeckt: [S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben und. [S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein Diese Steuerung ist immer noch Teil von NIST SP 800-53 Rev. 5.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. April 2024	[S3.11] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein	Security Hub hat dieses Steuerelement aus AWS Foundational Security Best Practices und Service-Managed Standard entfernt:. AWS Control Tower Es gibt zwar einige Fälle, in denen Ereignisbenachrichtigungen für S3-Buckets nützlich sind, dies ist jedoch keine allgemein bewährte Sicherheitsmethode. Diese Steuerung ist immer noch Teil von NIST SP 800-53 Rev. 5.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. April 2024	[SNS.1] SNS-Themen sollten im Ruhezustand wie folgt verschlüsselt werden AWS KMS	Security Hub hat dieses Steuerelement aus AWS Foundational Security Best Practices und Service-Managed Standard entfernt:. AWS Control Tower Da SNS Themen bereits standardmäßig verschlüsselt, wird die Verwendung AWS KMS zur Verschlüsselung von Themen als bewährte Sicherheitsmethode nicht mehr empfohlen. Dieses Steuerelement ist immer noch Teil von NIST SP 800-53 Rev. 5.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
8. April 2024	[ELB.6] Für Anwendungen, Gateways und Network Load Balancers sollte der Löschschutz aktiviert sein	Der Steuerelementtitel wurde von Applicati on Load Balancer Balancer-Löschschu tz aktiviert in Applicati on, Gateway und Network Load Balancer sollten den Löschschutz aktiviert haben geändert. Dieses Steuerele ment bewertet derzeit Application, Gateway und Network Load Balancer. Der Titel und die Beschreibung wurden geändert, um das aktuelle Verhalten genau widerzusp iegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
22. März 2024	[Opensearch.8] Verbindungen zu OpenSearch Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden	Der Titel des Steuerelements wurde von Verbindungen zu OpenSearch Domänen sollten mit TLS 1.2 verschlüsselt werden in Verbindungen zu OpenSearch Domänen sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden geändert. Bisher überprüfte das Steuerelement nur, ob Verbindungen zu OpenSearch Domänen TLS 1.2 verwendeten. Das Steuerelement stellt nun `PASSED` fest, ob OpenSearch Domänen mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt wurden. Der Titel und die Beschreibung des Steuerelements wurden aktualisiert, um das aktuelle Verhalten widerzuspiegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
22. März 2024	[ES.8] Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden	Der Titel des Steuerelements wurde von Connections zu Elasticsearch-Domains sollte mit TLS 1.2 verschlüsselt werden. Verbindungen zu Elasticsearch-Domains sollten mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt werden. Bisher überprüfte das Steuerelement nur, ob Verbindungen zu Elasticsearch-Domains TLS 1.2 verwendeten. Das Steuerelement stellt nun `PASSED` fest, ob Elasticsearch-Domains mit der neuesten TLS-Sicherheitsrichtlinie verschlüsselt wurden. Der Titel und die Beschreibung des Steuerelements wurden aktualisiert, um das aktuelle Verhalten widerzuspiegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.1] Bei S3-Allzweck-Buckets sollten die Einstellungen für den öffentlichen Zugriff blockieren aktiviert sein	Der Titel sollte von der Einstellung „Öffentlichen Zugriff blockieren“ auf die Einstellung „Öffentlichen Zugriff blockieren“ in S3-Allzweck-Buckets geändert werden. Security Hub hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.2] S3-Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren	Der geänderte Titel von S3-Buckets sollte den öffentlichen Lesezugriff auf S3-Buckets verbieten . Allzweck-Buckets sollten den öffentlichen Lesezugriff blockieren. Security Hub hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.3] S3-Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren	Der geänderte Titel von S3-Buckets sollte den öffentlichen Schreibzugriff auf S3-Buckets verbieten . Allzweck-Buckets sollten den öffentlichen Schreibzugriff blockieren. Security Hub hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.5] S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern	Die Änderung des Titels von S3-Buckets sollte Anfragen zur Verwendung von Secure Socket Layer erfordern, zu S3-Allzweck-Buckets sollten Anfragen zur Verwendung von SSL erfordern. Security Hub hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten	Der geänderte Titel von S3-Berechtigungen, die anderen AWS-Konten in Bucket-Richtlinien gewährt wurden, sollte auf S3-Allzweck-Bucket-Richtlinien beschränkt werden, sollten den Zugriff auf andere einschränken AWS-Konten. Security Hub hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden	Bei der Änderung des Titels von S3-Buckets sollte die regionsübergreifende Replikation aktiviert sein, sodass für S3-Buckets für allgemeine Zwecke die regionsübergreifende Replikation verwendet werden sollte. Security Hub hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden	Bei der Änderung des Titels von S3-Buckets sollte die regionsübergreifende Replikation aktiviert sein, sodass für S3-Buckets für allgemeine Zwecke die regionsübergreifende Replikation verwendet werden sollte. Security Hub hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.8] S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren	Der Titel sollte von der Einstellung S3-Zugriff blockieren auf Bucket-Ebene zu S3-Allzweck-Buckets sollten den öffentlichen Zugriff blockieren. Security Hub hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.9] Bei S3-Allzweck-Buckets sollte die Serverzugriffsprotokollierung aktiviert sein	Der Titel wurde von der Protokollierung des S3-Bucket-Serverzugriffs aktiviert in die Serverzug riffsprotokollierung sollte für S3-Allzweck-Buckets aktiviert sein geändert. Security Hub hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.10] S3-Allzweck-Buckets mit aktivierter Versionierung sollten Lifecycle-Konfigurationen haben	Bei der Änderung des Titels von S3-Buckets mit aktiviert er Versionierung sollten Lebenszyk lusrichtlinien so konfiguriert sein, dass S3-Allzweck-Buckets mit aktiviert er Versionierung Lifecycle-Konfigur ationen haben sollten. Security Hub hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.11] Bei S3-Allzweck-Buckets sollten Ereignisbenachrichtigungen aktiviert sein	Bei der Änderung des Titels von S3-Buckets sollten Ereignisbenachrichtigungen aktiviert sein, bei S3-Buckets für allgemeine Zwecke sollten Ereignisbenachrichtigungen aktiviert sein. Security Hub hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.12] ACLs sollten nicht verwendet werden, um den Benutzerzugriff auf S3-Allzweck-Buckets zu verwalten	Der geänderte Titel von S3-Zugriffskontrollisten (ACLs) sollte nicht zur Verwaltung des Benutzerzugriffs auf Buckets verwendet werden. ACLs sollten nicht zur Verwaltung des Benutzerzugriffs auf S3-Allzweck-Buckets verwendet werden. Security Hub hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.13] S3-Allzweck-Buckets sollten Lifecycle-Konfigurationen haben	Bei der Änderung des Titels von S3-Buckets sollten die Lebenszyklusrichtlinien so konfiguriert sein, dass S3-Allzweck-Buckets Lifecycle-Konfigurationen haben sollten. Security Hub hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.14] Für S3-Allzweck-Buckets sollte die Versionierung aktiviert sein	Bei der Änderung des Titels von S3-Buckets sollte Versionierung verwendet werden, bei S3-Buckets für allgemeine Zwecke sollte die Versionierung aktiviert sein. Security Hub hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
12. März 2024	[S3.15] Bei S3-Allzweck-Buckets sollte Object Lock aktiviert sein	Der geänderte Titel von S3-Buckets sollte so konfiguriert werden, dass Object Lock verwendet wird. Für S3-Allzweck-Buckets sollte Object Lock aktiviert sein. Security Hub hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.
12. März 2024	[S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys	Der Titel wurde von S3-Buckets sollten im Ruhezustand mit AWS KMS keys verschlüsselt werden in S3-Buckets für allgemeine Zwecke geändert. AWS KMS keys Security Hub hat den Titel geändert, um einen neuen S3-Bucket-Typ zu berücksichtigen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
7. März 2024	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub unterstützt jetzt `nodejs20.x` und `ruby3.3` als Parameter.
22. Februar 2024	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub unterstützt jetzt `dotnet8` als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
5. Februar 2024	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Security Hub hat die älteste unterstützte Version von Kubernetes, auf der der Amazon EKS-Cluster ausgeführt werden kann, aktualisiert, um ein bestehendes Ergebnis zu erzielen. Die derzeit älteste unterstützte Version ist Kubernetes `1.25`.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
10. Januar 2024	[CodeBuild.1] Die URLs des CodeBuild Bitbucket-Quell-Repositorys sollten keine vertraulichen Anmeldeinformationen enthalten	Geänderte Titel- URLs CodeBuild GitHub oder Bitbucket -Quell-Repository- URLs sollten OAuth verwenden, sodass CodeBuild Bitbucket -Quell-Repository- URLs keine vertrauli chen Anmeldein formationen enthalten sollten. Security Hub hat die Erwähnung von OAuth entfernt, da auch andere Verbindungsmethode n sicher sein können. Security Hub hat die Erwähnung von entfernt GitHub , da es nicht mehr möglich ist, ein persönliches Zugriffstoken oder einen Benutzernamen und ein Passwort in den GitHub Quell- Repository-URLs zu haben.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
8. Januar 2024	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub unterstützt `go1.x` und nicht mehr `java8` als Parameter, da es sich dabei um ausgemusterte Laufzeiten handelt.
29. Dezember 2023	[RDS.8] Für RDS-DB-Instances sollte der Löschschutz aktiviert sein	RDS.8 prüft, ob für eine Amazon RDS-DB-Instance, die eine der unterstützten Datenbank-Engines verwendet, der Löschschutz aktiviert ist. Security Hub unterstützt jetzt `custom-oracle-eeoracle-ee-cdb` , und `oracle-se2-cdb` als Datenbank-Engines.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
22. Dezember 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub unterstützt jetzt `java21` und `python3.12` als Parameter. Security Hub unterstützt nicht mehr `ruby2.7` als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
15. Dezember 2023	Bei [CloudFront.1] CloudFront Distributionen sollte ein Standard-Root-Objekt konfiguriert sein	CloudFront.1 prüft, ob für eine CloudFront Amazon-Distribution ein Standard-Root-Objekt konfiguriert ist. Security Hub hat den Schweregrad dieser Kontrolle von CRITICAL auf HIGH herabgesetzt, da das Hinzufügen des Standard-Root-Objekts eine Empfehlung ist, die von der Anwendung und den spezifischen Anforderungen des Benutzers abhängt.
05. Dezember 2023	[EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen	Der Titel des Steuerelements wurde von Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 auf Port 22 zulassen in Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 22 zulassen geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
05. Dezember 2023	[EC2.14] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulassen	Der Kontrolltitel wurde von „Sicherstellen, dass keine Sicherheitsgruppen den Zugriff von 0.0.0.0/0 auf Port 3389 zulassen“ in „Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 oder: :/0 auf Port 3389 zulassen“ geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
05. Dezember 2023	[RDS.9] RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch	Der Kontrolltitel wurde von Datenbank protokollierung sollte aktiviert sein in RDS-DB-Instances geändert, sodass RDS-DB-Instances Protokolle in Logs veröffentlichen sollten. CloudWatch Security Hub hat festgestellt, dass dieses Steuerelement nur prüft, ob Protokolle in Amazon CloudWatch Logs veröffentlicht werden, und nicht, ob RDS-Protokolle aktiviert sind. Das Steuerelement stellt PASSED fest, ob RDS-DB-Instances so konfiguriert sind, dass sie CloudWatch Protokolle in Logs veröffentlichen. Der Titel des Steuerelements wurde aktualisiert, um das aktuelle Verhalten widerzuspiegeln.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
17. November 2023	[EC2.19] Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen	EC2.19 prüft, ob uneingeschränkter eingehender Verkehr für eine Sicherheitsgruppe für die angegebenen Ports, die als risikoreich gelten, zugänglich ist. Security Hub hat dieses Steuerelement aktualisiert, um verwaltete Präfixlisten zu berücksichtigen, wenn sie als Quelle für eine Sicherheitsgruppenregel bereitgestellt werden. Das Steuerelement ermittelt, ob `FAILED` die Präfixlisten die Zeichenketten '0.0.0.0/0' oder ': :/0' enthalten.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. November 2023	[CloudWatch.15] Für CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein	Der Titel des Steuerelements wurde von „CloudWatch Alarme sollte eine Aktion für den ALARM-Status konfigurieren“ zu „ CloudWatch Alarme sollten bestimmte Aktionen konfiguriert haben“ geändert.
16. November 2023	[CloudWatch.16] CloudWatch Protokoll gruppen sollten für einen bestimmten Zeitraum aufbewahrt werden	Der geänderte Kontrolltitel aus CloudWatch Protokoll gruppen sollte mindestens ein Jahr lang aufbewahrt werden, während CloudWatch Protokoll gruppen für einen bestimmten Zeitraum aufbewahrt werden sollten.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. November 2023	[Lambda.5] VPC-Lambda-Funktionen sollten in mehreren Availability Zones funktionieren	Der Titel der Steuerung wurde von VPC-Lambda-Funktionen sollten in mehr als einer Availability Zone funktionieren, in VPC-Lambda-Funktionen geändert, die in mehreren Availability Zones funktionieren sollten.
16. November 2023	[AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben	Der Titel des Steuerelements wurde von AWS AppSync sollte die Protokollierung auf Anfrage- und Feldebene aktiviert haben in Die Protokollierung auf Feldebene sollte aktiviert sein geändert.AWS AppSync

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. November 2023	[EMR.1] Primäre Amazon EMR-Clusterknoten sollten keine öffentlichen IP-Adressen haben	Der Kontrolltitel wurde von Amazon Elastic MapReduce Cluster-Masterknoten sollten keine öffentlichen IP-Adressen haben zu Amazon EMR-Cluster-Primärknoten sollten keine öffentlic hen IP-Adressen haben.
16. November 2023	[Opensearch.2] OpenSearch -Domains sollten nicht öffentlich zugänglich sein	Der Titel der Steuerung wurde von OpenSearch Domänen, die sich in einer VPC befinden sollten, zu OpenSearc hDomänen geändert, die nicht öffentlic h zugänglich sein sollten.
16. November 2023	[ES.2] Elasticsearch-Domains sollten nicht öffentlich zugänglich sein	Der Titel des Steuerelements wurde von Elasticse arch-Domains in einer VPC geändert und Elasticsearch-Domains sollten nicht öffentlich zugänglich sein.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
31. Oktober 2023	[ES.4] Die Elasticsearch-Domain-Fehlerprotokollierung in CloudWatch Logs sollte aktiviert sein	ES.4 prüft, ob Elasticsearch-Domains so konfiguriert sind, dass sie Fehlerprotokolle an Amazon CloudWatch Logs senden. Die Kontrolle ergab zuvor einen PASSED Befund für eine Elasticsearch-Domain, deren Logs so konfiguriert sind, dass sie an Logs gesendet werden. CloudWatch Security Hub hat das Steuerelement aktualisiert, sodass nur Ergebnisse für PASSED eine Elasticsearch-Domain generiert werden, die so konfiguriert ist, dass sie CloudWatch Fehlerprotokolle an Logs sendet. Das Steuerelement wurde außerdem aktualisiert, um Elasticsearch-Versionen, die Fehlerprotokolle nicht unterstützen, von der Auswertung auszuschließen.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. Oktober 2023	[EC2.13] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 22 zulassen	EC2.13 prüft, ob Sicherheitsgruppen uneingeschränkten Eingangszugriff auf Port 22 zulassen. Security Hub hat dieses Steuerelement aktualisiert, um verwaltete Präfixlisten zu berücksichtigen, wenn sie als Quelle für eine Sicherheitsgruppenregel bereitgestellt werden. Das Steuerelement ermittelt, ob `FAILED` die Präfixlisten die Zeichenketten '0.0.0.0/0' oder ': :/0' enthalten.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. Oktober 2023	[EC2.14] Sicherheitsgruppen sollten keinen Zugang von 0.0.0.0/0 oder: :/0 zu Port 3389 zulassen	EC2.14 prüft, ob Sicherheitsgruppen uneingeschränkten Eingangszugriff auf Port 3389 zulassen. Security Hub hat dieses Steuerelement aktualisiert, um verwaltete Präfixlisten zu berücksichtigen, wenn sie als Quelle für eine Sicherheitsgruppenregel bereitgestellt werden. Das Steuerelement ermittelt, ob `FAILED` die Präfixlisten die Zeichenketten '0.0.0.0/0' oder ': :/0' enthalten.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. Oktober 2023	[EC2.18] Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Datenverkehr für autorisierte Ports zulassen	EC2.18 prüft, ob die verwendeten Sicherheitsgruppen uneingeschränkten eingehenden Verkehr zulassen. Security Hub hat dieses Steuerelement aktualisiert, um verwaltete Präfixlisten zu berücksichtigen, wenn sie als Quelle für eine Sicherhei tsgruppenregel bereitgestellt werden. Das Steuerelement ermittelt, ob `FAILED` die Präfixlisten die Zeichenketten '0.0.0.0/0' oder ': :/0' enthalten.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
16. Oktober 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub unterstützt jetzt `python3.11` als Parameter.
04. Oktober 2023	[S3.7] S3-Allzweck-Buckets sollten die regionsübergreifende Replikation verwenden	Security Hub hat den Parameter `ReplicationType` mit dem Wert von hinzugefügt, `CROSS-REGION` um sicherzustellen, dass bei S3-Buckets die regionsübergreifende Replikation aktiviert ist und nicht die Replikation derselben Region.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
27. September 2023	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	Security Hub hat die älteste unterstützte Version von Kubernetes, auf der der Amazon EKS-Cluster ausgeführt werden kann, aktualisiert, um ein bestehendes Ergebnis zu erzielen. Die derzeit älteste unterstützte Version ist Kubernetes `1.24`.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. September 2023	CloudFront.2 — Bei CloudFront Distributionen sollte die Origin-Zugriffsidentität aktiviert sein	Security Hub hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Folgen Sie stattdessen der Anleitung unter [CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden. Die Zugriffskontrolle von Origin ist derzeit die bewährte Methode im Bereich Sicherheit. Diese Kontrolle wird in 90 Tagen aus der Dokumentation entfernt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. September 2023	[EC2.22] Ungenutzte Amazon EC2-Sicherheitsgruppen sollten entfernt werden	Security Hub hat dieses Steuerelement aus AWS Foundational Security Best Practices (FSBP) und SP 800-53 Rev. 5 des National Institute of Standards and Technology (NIST) entfernt. Es ist immer noch Teil des Service-Managed Standard:. AWS Control Tower Dieses Steuerelement führt zu einer bestandenen Feststellung, ob Sicherheitsgruppen an EC2-Instances oder an eine elastic network interface angehängt sind. In bestimmten Anwendungsfällen stellen nicht verknüpfte Sicherheitsgruppen jedoch kein Sicherheitsrisiko dar. Sie können andere EC2-Steuerelemente wie EC2.2, EC2.13, EC2.14, EC2.18 und EC2.19 verwenden, um Ihre

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
		Sicherheitsgruppen zu überwachen.
20. September 2023	EC2.29 — EC2-Instances sollten in einer VPC gestartet werden	Security Hub hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Amazon EC2 hat EC2-Classic-Instances zu einer VPC migriert. Diese Kontrolle wird in 90 Tagen aus der Dokumentation entfernt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. September 2023	S3.4 — Bei S3-Buckets sollte die serverseitige Verschlüsselung aktiviert sein	Security Hub hat dieses Steuerelement entfernt und es aus allen Standards entfernt. Amazon S3 bietet jetzt Standardverschlüsselung mit verwalteten S3-Schlüsseln (SS3-S3) für neue und bestehende S3-Buckets. Die Verschlüsselungseinstellungen für bestehende Buckets, die mit serverseitiger SS3-S3- oder SS3-KMS-Verschlüsselung verschlüsselt sind, sind unverändert. Dieses Steuerelement wird in 90 Tagen aus der Dokumentation entfernt.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[EC2.2] VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen	Der Titel des Steuerelements wurde von Die VPC-Standardsicherheitsgruppe sollte keinen eingehenden und ausgehenden Datenverkehr zulassen zu VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Datenverkehr zulassen geändert.
14. September 2023	[IAM.9] MFA sollte für den Root-Benutzer aktiviert sein	Der Steuertitel wurde von Virtual MFA sollte für den Root-Benutzer aktiviert sein zu MFA sollte für den Root-Benutzer aktiviert sein geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[RDS.19] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Cluster-Ereignisse konfiguriert werden	Der Titel des Steuerelements wurde von Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Clusterereignisse konfiguriert werden in Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Clusterereignisse konfiguriert werden geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[RDS.20] Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Ereignisse der Datenbankinstanz konfiguriert werden	Der Titel des Steuerelements wurde von Ein Abonnement für RDS-Ereignisbenachrichtigungen sollte für kritische Datenbankinstanzereignisse konfiguriert werden in Bestehende Abonnements für RDS-Ereignisbenachrichtigungen sollten für kritische Datenbankinstanzereignisse konfiguriert werden geändert.
14. September 2023	[WAF.2] AWS WAF Klassische Regionalregeln sollten mindestens eine Bedingung haben	Der Titel des Steuerelements wurde von „Eine WAF-Regionalregel sollte mindestens eine Bedingung haben“ in „AWS WAF Klassische regionale Regeln“ geändert, die mindestens eine Bedingung haben sollten.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[WAF.3] AWS WAF Klassische regionale Regelgruppen sollten mindestens eine Regel haben	Der Kontrolltitel wurde von einer regionale n WAF-Regelgruppe sollte mindestens eine Regel enthalten zu einer AWS WAF klassischen regionalen Regelgrup pe geändert, die mindestens eine Regel haben sollte.
14. September 2023	[WAF.4] AWS WAF Klassische regionale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben	Der Kontrolltitel wurde von Eine regionale WAF-Web-ACL sollte mindesten s eine Regel oder Regelgruppe haben in AWS WAF Klassisch e regionale Web-ACLs geändert, die mindestens eine Regel oder Regelgrup pe haben sollten.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[WAF.6] AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben	Der Titel des Steuerelements wurde von „Eine globale WAF-Regel sollte mindestens eine Bedingung haben“ zu „AWS WAF Klassische globale Regeln sollten mindestens eine Bedingung haben“ geändert.
14. September 2023	[WAF.7] AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben	Der Titel des Steuerelements wurde von „Eine globale WAF-Regelgruppe sollte mindestens eine Regel haben“ zu „AWS WAF Klassische globale Regelgruppen sollten mindestens eine Regel haben“ geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
14. September 2023	[WAF.8] AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben	Der Steuerelementtitel wurde von Eine globale WAF-Web-ACL sollte mindestens eine Regel oder Regelgruppe haben in AWS WAF Klassische globale Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben geändert.
14. September 2023	[WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben	Der Kontrolltitel wurde von „Eine WAFv2-Web-ACL sollte mindestens eine Regel oder Regelgruppe haben“ zu „AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben“ geändert.
14. September 2023	[WAF.11] Die AWS WAF Web-ACL-Protokollierung sollte aktiviert sein	Der Kontrolltitel wurde von AWS WAF v2-Web-ACL-Protokollierung in AWS WAF Web-ACL-Protokollierung sollte aktiviert sein geändert.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. Juli 2023	S3.4 — Bei S3-Buckets sollte die serverseitige Verschlüsselung aktiviert sein	S3.4 prüft, ob für einen Amazon S3 S3-Bucket entweder die serverseitige Verschlüsselung aktiviert ist oder ob die S3-Bucket-Richtlinie `PutObject` Anfragen ohne serverseitige Verschlüsselung explizit ablehnt. Security Hub hat diese Steuerung aktualisiert und umfasst nun eine serverseitige Dual-Layer-Verschl üsselung mit KMS-Schlüsseln (DSSE-KMS). Wenn ein S3-Bucket mit SSE-S3, SSE-KMS oder DSSE-KMS verschlüs selt ist, gibt das Steuerelement ein passendes Ergebnis aus.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
17. Juli 2023	[S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys	S3.17 prüft, ob ein Amazon S3 S3-Bucket mit einem verschlüsselt ist. AWS KMS key Security Hub hat diese Steuerung aktualisiert und umfasst nun eine serverseitige Dual-Layer-Verschlüsselung mit KMS-Schlüsseln (DSSE-KMS). Wenn ein S3-Bucket mit SSE-KMS oder DSSE-KMS verschlüsselt ist, gibt das Steuerelement ein passendes Ergebnis aus.
9. Juni 2023	[EKS.2] EKS-Cluster sollten auf einer unterstützten Kubernetes-Version ausgeführt werden	EKS.2 prüft, ob ein Amazon EKS-Cluster auf einer unterstützten Kubernetes-Version läuft. Die älteste unterstützte Version ist jetzt `1.23`

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
9. Juni 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub unterstützt jetzt `ruby3.2` als Parameter.
5. Juni 2023	[ApiGateway.5] API Gateway REST API-Cache-Daten sollten im Ruhezustand verschlüsselt werden	ApiGateway.5. Überprüft, ob alle Methoden in den REST-API-Stufen von Amazon API Gateway im Ruhezustand verschlüsselt sind. Security Hub hat das Steuerelement aktualisiert, sodass die Verschlüsselung einer bestimmten Methode nur ausgewertet wird, wenn das Caching für diese Methode aktiviert ist.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
18. Mai 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub unterstützt jetzt `java17` als Parameter.
18. Mai 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub unterstützt nicht mehr `nodejs12.x` als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
23. April 2023	[ECS.10] Die ECS Fargate-Dienste sollten auf der neuesten Fargate-Plattformversion laufen	ECS.10 prüft, ob die Amazon ECS Fargate-Dienste die neueste Fargate-Plattformversion ausführen. Kunden können Amazon ECS direkt über ECS oder mithilfe von ECS bereitstellen CodeDeploy. Security Hub hat dieses Steuerelement aktualisiert, sodass bei der Bereitstellung von ECS Fargate-Diensten CodeDeploy die Ergebnisse „Bestanden“ angezeigt werden.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
20. April 2023	[S3.6] Allgemeine S3-Bucket-Richtlinien sollten den Zugriff auf andere einschränken AWS-Konten	S3.6 prüft, ob eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) verhindert, dass Prinzipale AWS-Konten anderer Benutzer verweigerte Aktionen für Ressourcen im S3-Bucket ausführen. Security Hub hat die Steuerung aktualisiert, um Bedingungen in einer Bucket-Richtlinie zu berücksichtigen.
18. April 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub unterstützt jetzt `python3.10` als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
18. April 2023	[Lambda.2] Lambda-Funktionen sollten unterstützte Laufzeiten verwenden	Lambda.2 prüft, ob die AWS Lambda Funktionseinstellungen für Laufzeiten mit den erwarteten Werten übereinstimmen, die für die unterstützten Laufzeiten in jeder Sprache festgelegt wurden. Security Hub unterstützt nicht mehr `dotnetcore3.1` als Parameter.

Datum der Änderung	Kontroll-ID und Titel	Beschreibung der Änderung
17. April 2023	[RDS.11] Bei RDS-Instances sollten automatische Backups aktiviert sein	RDS.11 prüft, ob für Amazon RDS-Instances automatische Backups aktiviert sind, wobei die Aufbewahrungsdauer für Backups mindestens sieben Tage beträgt. Security Hub hat diese Kontrolle aktualisiert, um Read Replicas von der Evaluierung auszuschließen, da nicht alle Engines automatische Backups auf Read Replicas unterstützen. Darüber hinaus bietet RDS nicht die Möglichkeit, bei der Erstellung von Read Replicas einen Aufbewahrungszeitraum für Backups festzulegen. Read Replicas werden standardmäßig mit einer Aufbewahrungsdauer für Backups erstellt. `0`

Dokumentenverlauf für das AWS Security Hub Hub-Benutzerhandbuch

In der folgenden Tabelle werden die Aktualisierungen der Dokumentation für AWS Security Hub beschrieben.

> **Note**
>
> Bei Sicherheitskontrollen ist das angegebene Datum das Datum, an dem die Kontrollen in allen Konten und Regionen verfügbar sind. Es kann 1—2 Wochen dauern, bis die Kontrollen alle Konten und Regionen erreichen.

Änderung	Beschreibung	Datum
Veröffentlichung von CIS AWS Foundations Benchmark v3.0.0	Security Hub hat den Center for Internet Security (CIS) AWS Foundations Benchmark v3.0.0 veröffentlicht. Die Version enthält die folgenden neuen Steuerelemente sowie Zuordnungen zu mehreren vorhandenen Steuerele menten. • the section called “[EC2.53] EC2-Sicherheitsgruppen sollten keinen Zugriff von 0.0.0.0/0 zu Remote-Serververwaltungsports zulassen” • the section called “[EC2.54] EC2-Sicherheitsgruppen sollten keinen Zugang von: :/0 zu Remote-Se	13. Mai 2024

rveradministrationsports zulassen”

- the section called “[IAM.26] Abgelaufene SSL/TLS-Zertifikate, die in IAM verwaltet werden, sollten entfernt werden”
- the section called “[IAM.27] IAM-Identitäten sollte die Richtlinie nicht angehängt sein AWSCloudShellFullAccess ”
- the section called “[IAM.28] Der externe Zugriffsanalysator für IAM Access Analyzer sollte aktiviert sein”
- the section called “[S3.22] S3-Allzweck-Buckets sollten Schreibereignisse auf Objektebene protokollieren”
- the section called “[S3.23] S3-Allzweck-Buckets sollten Leseereignisse auf Objektebene protokollieren”

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub-Steuerelemente sind verfügbar: • the section called “[DataFirehose.1] Firehose-Lieferstreams sollten im Ruhezustand verschlüsselt werden” • the section called “[DMS.10] Auf DMS-Endpunkten für Neptune-Datenbanken sollte die IAM-Autorisierung aktiviert sein” • the section called “[DMS.11] Bei DMS-Endpunkten für MongoDB sollte ein Authentifizierungsmechanismus aktiviert sein” • the section called “[DMS.12] Auf DMS-Endpunkten für Redis sollte TLS aktiviert sein” • the section called “[DynamoDB.7] DynamoDB Accelerator-Cluster sollten bei der Übertragung verschlüsselt werden” • the section called “[EFS.6] EFS-Mount-Ziele sollten keinem öffentlichen Subnetz zugeordnet werden” • the section called “[EKS.3] EKS-Cluster sollten verschlüsselte Kubernetes-Geheimnisse verwenden”	3. Mai 2024

- the section called “[FSX.2] FSx for Lustre-Dateisysteme sollten so konfiguriert sein, dass Tags in Backups kopiert werden”
- the section called “[MQ.2] ActiveMQ-Broker sollten Audit-Logs streamen an CloudWatch”
- the section called “[MQ.3] Bei Amazon MQ-Broker n sollte das automatische Upgrade der Nebenversion aktiviert sein”
- the section called “[Opensearch.11] OpenSearch Domains sollten mindestens drei dedizierte Primärknoten haben”
- the section called “[Redshift.15] Redshift-Sicherheitsgruppen sollten den Zugriff auf den Cluster-Port nur von eingeschränkten Quellen zulassen”
- the section called “[SageMaker.4] Bei Produktionsvarianten für SageMaker Endgeräte sollte die anfängliche Anzahl der Instances größer als 1 sein”
- the section called “[ServiceCatalog.1] Servicekatalog-Portfolios sollten nur innerhalb einer AWS

	Organisation gemeinsam genutzt werden” • the section called “[Transfer.2] Transfer Family Family-Server sollten kein FTP-Protokoll für die Endpunktverbindung verwenden”	
AWS Standard für die Kennzeichnung von Ressourcen	Der AWS Resource Tagging Standard von Security Hub ist jetzt allgemein verfügbar , zusammen mit neuen Kontrollen, die für den Standard gelten.	30. April 2024
Aktualisierung der bestehenden verwalteten Richtlinie	Security Hub AWS hat die verwaltete Richtlinie mit dem Namen aktualisiert`AmazonSecurityHubFullAccess` , um Preisdetails für AWS-Services und Produkte abzurufen.	24. April 2024
Konfiguration der Steuerparameter im Kontext	Wenn Sie die zentrale Konfiguration verwenden , können Sie Steuerung sparameter jetzt kontextbezogen auf der Detailseite eines Steuerelements auf der Security Hub Hub-Konsole konfigurieren.	29. März 2024
Aktualisierung der bestehenden verwalteten Richtlinie	Security Hub AWS hat die verwaltete Richtlinie aktualisiert, `AWSSecurityHubReadOnlyAccess` indem sie ein `Sid` Feld hinzugefügt hat.	22. Februar 2024

Neue Sicherheitskontrolle	Das Steuerelement [Macie.2] Die automatische Erkennung sensibler Daten durch Macie sollte aktiviert sein, ist jetzt verfügbar. Informationen zu regionalen Beschränkungen für dieses Steuerelement finden Sie unter Verfügbarkeit von Steuerelementen nach Regionen.	19. Februar 2024
Security Hub in Kanada West (Calgary) verfügbar	Security Hub ist jetzt in Canada West (Calgary) verfügbar. Alle Security Hub Hub-Funktionen sind jetzt in dieser Region verfügbar , mit Ausnahme bestimmter Sicherheitskontrollen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.	20. Dezember 2023

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub-Steuerelemente sind verfügbar: • the section called “[Backup.1] AWS Backup Wiederherstellungspunkte sollten im Ruhezustand verschlüsselt sein” • the section called “[DynamoDB.6] Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein” • the section called “[EC2.51] Bei EC2-Client-VPN-Endpunkten sollte die Client-Verbindungsprotokollierung aktiviert sein” • the section called “[EKS.8] Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein” • the section called “[EMR.2] Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein” • the section called “[FSX.1] FSx für OpenZFS-Dateisysteme sollte so konfiguriert sein, dass Tags auf Backups und Volumes kopiert werden”	14. Dezember 2023

- the section called “[Macie.1] Amazon Macie sollte aktiviert sein”
- the section called “[MSK.2] Für MSK-Cluster sollte die erweiterte Überwachung konfiguriert sein”
- the section called “[Neptune.9] Neptune-DB-Cluster sollten in mehreren Availability Zones bereitgestellt werden”
- the section called “[Network Firewall.1] Netzwerk-Firewall-Firewalls sollten in mehreren Availability Zones eingesetzt werden”
- the section called “[Network Firewall.2] Die Netzwerk-Firewall-Protokollierung sollte aktiviert sein”
- the section called “Auf [Opensearch.10] OpenSearch -Domains sollte das neueste Softwareupdate installiert sein”
- the section called “[PCA.1] AWS Private CA Root-Zertifizierungsstelle sollte deaktiviert sein”
- the section called “[S3.19] Bei S3-Zugriffspunkten sollten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sein”

	• the section called “[S3.20] Bei S3-Allzweck-Buckets sollte MFA Delete aktiviert sein”	
Bereicherung finden	Security Hub hat die neuen Suchfelder `AwsAccountName` `ApplicationArn` , und `ApplicationName` zum AWS Security Finding Format (ASFF) hinzugefügt.	8. November 2023
Verbesserungen am Übersichts-Dashboard	Sie können jetzt auf der Übersichtsseite der Security Hub Hub-Konsole auf weitere Dashboard-Widgets zugreifen , Dashboard-Filtersätze speichern, um sich schnell auf bestimmte Sicherheitsprobleme zu konzentrieren, und das Dashboard-Layout anpassen.	8. November 2023
Zentrale Konfiguration	Die zentrale Konfiguration ist jetzt verfügbar. Bei der zentralen Konfiguration kann der delegierte Security Hub-Administrator Security Hub, Standards und Kontrollen für mehrere Unternehmenskonten , Organisationseinheiten (OUs) und Regionen konfigurieren.	8. November 2023

Aktualisierungen der verwaltet en Richtlinie	Security Hub hat der `AWSSecurityHubServ iceRolePolicy` verwaltet en Richtlinie neue Berechtig ungen hinzugefügt, die es Security Hub ermöglichen, anpassbare Eigenschaften der Sicherheitskontrolle zu lesen und zu aktualisieren.	26. November 2023
Benutzerdefinierte Steuerung sparameter	Sie können jetzt Parameter werte für ausgewählte Security Hub-Steuerelemente anpassen. Dies kann dazu führen, dass die Ergebnisse für eine bestimmte Kontrolle Ihren Geschäftsanforderungen und Sicherheitserwartungen besser entsprechen.	26. November 2023
Aktualisierungen der verwaltet en Richtlinien	Security Hub hat die Richtlini en aktualisiert `AWSSecuri tyHubFullAccess` und `AWSSecurityHubOrga nizationsAccess` verwaltet, mit denen Sie die Funktionen von Security Hub bzw. die Integration mit nutzen können AWS Organizations.	16. November 2023

Bestehende Sicherheitskontrollen wurden zum Service-Managed Standard hinzugefügt: AWS Control Tower	Die folgenden vorhandenen Security Hub-Steuerelemente wurden dem Service-Managed Standard hinzugefügt: AWS Control Tower. • ACM.2 • AppSync5. • CloudTrail.6 • DMS.9 • DocumentDB DB.3 • DynamoDB.3 • EC2.23 • EKS.1 • ElastiCache3. • ElastiCache.4 • ElastiCache.5 • ElastiCache.6 • EventBridge3. • KMS.4 • Lambda.3 • MQ.5 • MQ.6 • MSK.1 • RDS.12 • RDS.15 • S 3,17	14. November 2023

Aktualisierungen der verwaltet en Richtlinie	Security Hub hat der `AWSSecurityHubServ iceRolePolicy` verwaltet en Richtlinie eine neue Tagging-Berechtigung hinzugefügt, die es Security Hub ermöglicht, Ressource n-Tags zu lesen, die sich auf Ergebnisse beziehen.	7. November 2023

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub-Steuerelemente sind verfügbar: • the section called “[AppSync .5] AWS AppSync GraphQL-APIs sollten nicht mit API-Schlüsseln authentifiziert werden” • the section called “[DMS.6] Für DMS-Replikationsin stanzen sollte das automatis che Upgrade der Nebenvers ionen aktiviert sein” • the section called “[DMS.7] Bei DMS-Replikationsau fgaben für die Zieldatenbank sollte die Protokollierung aktiviert sein” • the section called “[DMS.8] Bei DMS-Replikationsau fgaben für die Quelldate nbank sollte die Protokoll ierung aktiviert sein” • the section called “[DMS.9] DMS-Endpunkte sollten SSL verwenden” • the section called “[DocumentDB.3] Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein” • the section called “[DocumentDB.4] Amazon DocumentDB-Cluster sollten	10. Oktober 2023

Auditprotokolle in Logs veröffentlichen CloudWatch ”
-

- the section called “[DocumentDB.5] Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein”
- the section called “[ECS.9] ECS-Aufgabendefinitionen sollten über eine Protokollierungskonfiguration verfügen”
- the section called “[EventBridge.3] An EventBridge benutzerdefinierte Eventbusse sollte eine ressourcenbasierte Richtlinie angehängt werden”
- the section called “[EventBridge.4] Auf EventBridge globalen Endpunkten sollte die Ereignisreplikation aktiviert sein”
- the section called “[MSK.1] MSK-Cluster sollten bei der Übertragung zwischen Broker-Knoten verschlüsselt werden”
- the section called “[MQ.5] ActiveMQ-Broker sollten den Aktiv-/Standby-Bereitstellungsmodus verwenden”
- the section called “[MQ.6] RabbitMQ-Broker sollten

den Cluster-Bereitstellungsmodus verwenden”

- the section called “[Network Firewall.9] Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein”
- the section called “[RDS.34] Aurora MySQL-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch ”
-
- the section called “[RDS.35] Für RDS-DB-Cluster sollte das automatische Upgrade auf Nebenversionen aktiviert sein”
- the section called “[Route53.2] Öffentlich gehostete Route 53-Zonen sollten DNS-Abfragen protokollieren”
- the section called “Für [WAF.12] AWS WAF Regeln sollten Metriken aktiviert sein CloudWatch ”

Aktualisierungen der verwaltet en Richtlinie	Security Hub hat der `AWSSecurityHubServ iceRolePolicy` verwaltet en Richtlinie neue Organisat ionsaktionen hinzugefügt, die es Security Hub ermöglichen, Informationen zu Konten und Organisationseinheiten (OU) abzurufen. Wir haben auch neue Security Hub-Aktionen hinzugefügt, die es Security Hub ermöglichen, Dienstkon figurationen, einschließlich Standards und Kontrollen, zu lesen und zu aktualisieren.	27. September 2023

Bestehende Sicherheitskontrollen wurden zum Service-Managed Standard hinzugefügt: AWS Control Tower	Die folgenden vorhandenen Security Hub-Steuerelemente wurden dem Service-Managed Standard hinzugefügt: AWS Control Tower. • the section called “[Athena.1] Athena-Arbeitsgruppen sollten im Ruhezustand verschlüsselt werden” • the section called “[DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden” • the section called “[DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen” • the section called “[Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden” • the section called “[Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch” • the section called “[Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein”	26. September 2023

- the section called “[Neptune .4] Bei Neptune-DB-Cluster n sollte der Löschschutz aktiviert sein”
- the section called “[Neptune .5] Bei Neptune-DB-Cluster n sollten automatische Backups aktiviert sein”
- the section called “[Neptune .6] Neptune-DB-Cluster -Snapshots sollten im Ruhezustand verschlüsselt werden”
- the section called “[Neptune .7] Bei Neptune-DB-Cluster n sollte die IAM-Daten bankauthentifizierung aktiviert sein”
- the section called “[Neptune .8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren”
- the section called “[RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden”

Ansicht konsolidierter Kontrollen und konsolidierte Kontrollergebnisse verfügbar in AWS GovCloud (US)	Die Ansicht der konsolidierten Kontrollen und die konsolidierten Kontrollergebnisse sind jetzt in der verfügbar AWS GovCloud (US) Region. Auf der Seite „Kontrollen“ der Security Hub Hub-Konsole werden all Ihre Kontrollen standardübergreifend angezeigt. Jede Kontrolle hat standardübergreifend dieselbe Kontroll-ID. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erhalten Sie ein einziges Ergebnis pro Sicherheitsprüfung, auch wenn eine Kontrolle für mehrere aktivierte Standards gilt.	6. September 2023
Ansicht konsolidierter Kontrollen und konsolidierte Kontrollergebnisse sind in den Regionen Chinas verfügbar	Eine konsolidierte Kontrollübersicht und konsolidierte Kontrollergebnisse sind jetzt in den Regionen Chinas verfügbar. Auf der Seite „Kontrollen“ der Security Hub Hub-Konsole werden all Ihre Kontrollen standardübergreifend angezeigt. Jede Kontrolle hat standardübergreifend dieselbe Kontroll-ID. Wenn Sie konsolidierte Kontrollergebnisse aktivieren, erhalten Sie ein einziges Ergebnis pro Sicherheitsprüfung, auch wenn eine Kontrolle für mehrere aktivierte Standards gilt.	28. August 2023

Security Hub in der Region Israel (Tel Aviv) verfügbar	Security Hub ist jetzt in Israel (Tel Aviv) verfügbar. Alle Security Hub Hub-Funktionen sind jetzt in dieser Region verfügbar, mit Ausnahme bestimmter Sicherheitskontrollen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.	08. August 2023

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub-Steuerelemente sind verfügbar: • the section called “[Athena.1] Athena-Arbeitsgruppen sollten im Ruhezustand verschlüsselt werden” • the section called “[DocumentDB.1] Amazon DocumentDB-Cluster sollten im Ruhezustand verschlüsselt werden” • the section called “[DocumentDB.2] Amazon DocumentDB-Cluster sollten über eine angemessene Aufbewahrungsfrist für Backups verfügen” • the section called “[Neptune.1] Neptune-DB-Cluster sollten im Ruhezustand verschlüsselt werden” • the section called “[Neptune.2] Neptune-DB-Cluster sollten Audit-Logs in Logs veröffentlichen CloudWatch” • the section called “[Neptune.3] Neptune-DB-Cluster-Snapshots sollten nicht öffentlich sein” • the section called “[Neptune.4] Bei Neptune-DB-Cluster	28. Juli 2023

	n sollte der Löschschutz aktiviert sein” • the section called “[Neptune .5] Bei Neptune-DB-Cluster n sollten automatische Backups aktiviert sein” • the section called “[Neptune .6] Neptune-DB-Cluster -Snapshots sollten im Ruhezustand verschlüsselt werden” • the section called “[Neptune .7] Bei Neptune-DB-Cluster n sollte die IAM-Daten bankauthentifizierung aktiviert sein” • the section called “[Neptune .8] Neptune-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren” • the section called “[RDS.27] RDS-DB-Cluster sollten im Ruhezustand verschlüsselt werden”	
Neue Operatoren für Kriterien für Automatisierungsregeln	Sie können jetzt die Vergleich soperatoren CONTAINS und NOT_CONTAINS für die Zuordnung von Automatis ierungsregeln und Zeichenke ttenkriterien verwenden.	25. Juli 2023

Automatisierungsregeln	Security Hub bietet jetzt Automatisierungsregeln, die Ergebnisse auf der Grundlage der von Ihnen angegebenen Kriterien automatisch aktualisieren.	13. Juni 2023
Neue Integration von Drittanbietern	Snykist eine neue Drittanbieter-Integration, die Ergebnisse an Security Hub sendet.	12. Juni 2023

Bestehende Sicherheitskontrollen wurden dem Service-Managed Standard hinzugefügt: AWS Control Tower	Die folgenden vorhandenen Security Hub-Steuerelemente wurden dem Service-Managed Standard hinzugefügt: AWS Control Tower. • the section called “[Account.1] Sicherheitskontaktinformationen sollten bereitgestellt werden für AWS-Konto” • the section called “[ApiGateway.8] API Gateway Gateway-Routen sollten einen Autorisierungstyp angeben” • the section called “[ApiGateway.9] Die Zugriffsprotokollierung sollte für API Gateway V2 Stages konfiguriert sein” • the section called “[CodeBuild.3] CodeBuild S3-Protokolle sollten verschlüsselt sein” • the section called “[EC2.25] Amazon EC2 EC2-Startvorlagen sollten Netzwerkschnittstellen keine öffentlichen IPs zuweisen” • the section called “[ELB.1] Application Load Balancer sollte so konfiguriert sein, dass alle HTTP-Anfragen an HTTPS umgeleitet werden”	12. Juni 2023

- the section called “[Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden”
- the section called “[SageMaker.2] SageMaker Notebook-Instances sollten in einer benutzerdefinierten VPC gestartet werden”
- the section called “[SageMaker.3] Benutzer sollten keinen Root-Zugriff auf SageMaker Notebook-Instances haben”
- the section called “[WAF.10] AWS WAF Web-ACLs sollten mindestens eine Regel oder Regelgruppe haben”

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub-Steuerelemente sind verfügbar: • the section called “[ACM.2] Von ACM verwaltete RSA-Zertifikate sollten eine Schlüssellänge von mindestens 2.048 Bit verwenden” • the section called “[AppSync.2] AWS AppSync sollte die Protokollierung auf Feldebene aktiviert haben” • the section called “[CloudFront.13] CloudFront Distributionen sollten die Origin-Zugriffskontrolle verwenden” • the section called “[Elastic Beanstalk.3] Elastic Beanstalk sollte Logs streamen nach CloudWatch” • the section called “[S3.17] S3-Allzweck-Buckets sollten im Ruhezustand verschlüsselt werden mit AWS KMS keys” • the section called “[StepFunctions.1] Step Functions Functions-Zustandsmaschinen sollten die Protokollierung aktiviert haben”	6. Juni 2023

Security Hub im asiatisch-pazifischen Raum (Melbourne) verfügbar	Security Hub ist jetzt im asiatisch-pazifischen Raum (Melbourne) verfügbar. Alle Security Hub Hub-Funktionen sind jetzt in dieser Region verfügbar, mit Ausnahme bestimmter Sicherheitskontrollen. Weitere Informationen finden Sie unter Verfügbarkeit von Kontrollen nach Regionen.	25. Mai 2023
Verlauf finden	Security Hub kann jetzt den Verlauf eines Fundes in den letzten 90 Tagen verfolgen.	4. Mai 2023
Neue Sicherheitskontrollen	Die folgenden neuen Security Hub-Steuerelemente sind verfügbar: • the section called “[EKS.1] EKS-Cluster-Endpunkte sollten nicht öffentlich zugänglich sein” • the section called “[ELB.16] Application Load Balancers sollten mit einer Web-ACL verknüpft sein AWS WAF” • the section called “[Redshift.10] Redshift-Cluster sollten im Ruhezustand verschlüsselt werden” • the section called “[S3.15] Bei S3-Allzweck-Buckets sollte Object Lock aktiviert sein”	29. März 2023

Erweiterte Unterstützung für konsolidierte Kontrollergebnisse	Die automatisierte Sicherheitsreaktion auf AWS Version 2.0.0 unterstützt jetzt konsolidierte Kontrollergebnisse.	24. März 2023
Security Hub in neuer Version erhältlich AWS-Regionen	Security Hub ist jetzt im asiatisch-pazifischen Raum (Hyderabad), Europa (Spanien) und Europa (Zürich) verfügbar. In diesen Regionen gibt es Beschränkungen, welche Kontrollen verfügbar sind.	21. März 2023
Aktualisierung der verwalteten Richtlinie	Security Hub hat eine bestehende Berechtigung in der `AWSSecurityHubServiceRolePolicy` verwalteten Richtlinie aktualisiert.	17. März 2023

Neue Sicherheitskontrollen für den Standard NIST 800-53	Security Hub hat die folgenden Sicherheitskontrollen hinzugefügt, die für den NIST 800-53-Standard gelten: • the section called “[Account.2] AWS-Konten sollte Teil einer Organisation sein AWS Organizations” • the section called “[CloudWatch.15] Für CloudWatch Alarme sollten bestimmte Aktionen konfiguriert sein” • the section called “[CloudWatch.16] CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden” • the section called “[CloudWatch.17] CloudWatch Alarmaktionen sollten aktiviert sein” • the section called “[DynamoDB.4] DynamoDB-Tabellen sollten in einem Backup-Plan vorhanden sein” • the section called “[EC2.28] EBS-Volumes sollten durch einen Backup-Plan abgedeckt werden” • EC2.29 — EC2-Instances sollten in einer VPC gestartet werden (eingestellt)	03. März 2023

	• the section called “[RDS.26] RDS-DB-Instances sollten durch einen Backup-Plan geschützt werden” • the section called “[S3.14] Für S3-Allzweck-Bucket s sollte die Versionierung aktiviert sein” • the section called “[WAF.11] Die AWS WAF Web-ACL-P rotokollierung sollte aktiviert sein”	
Nationales Institut für Standards und Technologie (NIST) 800-53 Rev. 5	Security Hub unterstützt jetzt den Standard NIST 800-53 Rev. 5 mit mehr als 200 anwendbaren Sicherhei tskontrollen.	28. Februar 2023
Konsolidierte Kontrollen: Ergebnisse anzeigen und kontrollieren	Mit der Veröffentlichung der konsolidierten Kontrollansicht werden auf der Kontrolls eite der Security Hub Hub-Konsole all Ihre Kontrolle n standardübergreifend angezeigt. Jede Kontrolle hat standardübergreifend dieselbe Kontroll-ID. Wenn Sie konsolidierte Kontrolle rgebnisse aktivieren, erhalten Sie ein einziges Ergebnis pro Sicherheitsprüfung, auch wenn eine Kontrolle für mehrere aktivierte Standards gilt.	23. Februar 2023

Neue Sicherheitskontrollen	Die folgenden neuen Security Hub-Steuerelemente sind verfügbar. Für einige Kontrollen gelten regionale Einschränkungen. • the section called “[ElastiCache.1] Bei ElastiCache Redis-Clustern sollte das automatische Backup aktiviert sein” • the section called “[ElastiCache.2] ElastiCache Für Redis-Cache-Cluster sollte das auto Upgrade der Nebenversion aktiviert sein” • the section called “[ElastiCache.3] ElastiCache Für Redis-Replikationsgruppen sollte der automatische Failover aktiviert sein” • the section called “[ElastiCache.4] ElastiCache für Redis-Replikationsgruppen sollten im Ruhezustand verschlüsselt werden” • the section called “[ElastiCache.5] ElastiCache für Redis-Replikationsgruppen sollten bei der Übertragung verschlüsselt werden” • the section called “[ElastiCache.6] ElastiCache Für Redis-Replikationsgruppen	16. Februar 2023

	vor Version 6.0 sollte Redis AUTH verwendet werden” • the section called “[ElastiCache.7] ElastiCache Cluster sollten nicht die Standard-Subnetzgruppe verwenden”	
Neue ASFF-Felder	Security Hub wurde hinzugefügt ProductFields. ArchivalReasonsSecurity Hub ProductFields wurde hinzugefügt. ----SEP----:0/Description und. ArchivalReasons:0/Description ReasonCode und. AWS ----sep----:0/ in das Security Finding Format (ASFF).	8. Februar 2023
Neue ASFF-Felder	Security Hub hat Compliance hinzugefügt. AssociatedStandards und Compliance. SecurityControlId zum AWS Security Finding Format (ASFF).	31. Januar 2023
Details zur Sicherheitslücke sind jetzt verfügbar	Sie können jetzt in der Security Hub-Konsole Details zu Sicherheitslücken für Ergebnisse sehen, die Amazon Inspector an Security Hub sendet.	14. Januar 2023
Security Hub ist im Mittleren Osten (VAE) verfügbar	Security Hub ist jetzt im Mittleren Osten (VAE) verfügbar. Für einige Kontrollen gelten regionale Beschränkungen.	12. Januar 2023

Integration von Drittanbietern mit hinzugefügt MetricStream	Security Hub unterstützt jetzt die Integration von Drittanbietern MetricStream in allen Regionen außer China und AWS GovCloud (US).	11. Januar 2023
Das Limit für Unternehmenskonten wurde erhöht	Security Hub unterstützt jetzt bis zu 11.000 Mitgliedskonten für jedes Security Hub-Administratorkonto pro Region.	27. Dezember 2022
ElasticBeanstalk3. wurde zurückgesetzt	Security Hub hat die Kontrolle [ElasticBeanstalk.3] rückgängig gemacht, zu der Elastic Beanstalk in allen Regionen Logs CloudWatch vom FSBP-Standard streamen sollte.	21. Dezember 2022
Security Hub fügt neue Sicherheitskontrollen hinzu	Neue Security Hub-Steuerelemente sind für Kunden verfügbar, die den FSBP-Standard aktiviert haben. Für einige Kontrollen gelten regionale Einschränkungen.	15. Dezember 2022
Hinweise zu kommenden Funktionen	Security Hub plant die Veröffentlichung von zwei neuen Funktionen: konsolidierte Kontrollansicht und konsolidierte Kontrollergebnisse. Diese kommenden Funktionen können sich auf bestehende Workflows auswirken, die auf Feldern und Werten für die Suche nach Kontrollen basieren.	9. Dezember 2022

Amazon Security Lake-Integration jetzt verfügbar	Security Lake lässt sich jetzt in Security Hub integrieren, indem es die Ergebnisse von Security Hub empfängt.	29. November 2022
Support für Service-Managed Standard: AWS Control Tower	Security Hub unterstützt einen neuen Sicherheitsstandard namens Service-Managed Standard: AWS Control Tower. AWS Control Tower verwaltet diesen Standard.	28. November 2022
CIS AWS Foundations Benchmark v1.4.0 ist jetzt in chinesischen Regionen verfügbar	Security Hub unterstützt jetzt den Benchmark v1.4.0 der CIS AWS Foundations in den Regionen Chinas.	18. November 2022
Die Cloud-Integration von Jira Service Management ist jetzt verfügbar	Jira Service Management Cloud empfängt jetzt Security Hub Hub-Ergebnisse in allen verfügbaren Regionen mit Ausnahme der Regionen China.	17. November 2022
AWS IoT Device Defender Integration jetzt verfügbar	AWS IoT Device Defender sendet jetzt Ergebnisse an Security Hub in allen verfügbaren Regionen.	17. November 2022
Support für CIS AWS Foundations Benchmark v1.4.0	Security Hub bietet jetzt Sicherheitskontrollen, die CIS AWS Foundations Benchmark v1.4.0 unterstützen. Dieser Standard ist in allen verfügbaren Regionen mit Ausnahme der Regionen China verfügbar.	9. November 2022

Support für Security Hub Hub-Ankündigungen in AWS GovCloud (US)	Sie können jetzt Security Hub-Ankündigungen mit Amazon Simple Notification Service (Amazon SNS) in (USA-Ost) und AWS GovCloud AWS GovCloud (US-West) abonnieren, um Benachric htigungen über Security Hub zu erhalten.	3. Oktober 2022
AWS Security Hub fügt eine neue Sicherheitskontrolle hinzu	Das neue Security Hub Control AutoScaling.9 steht Kunden zur Verfügung, die den FSBP-Standard aktiviert haben. Die Kontrollen können regionalen Einschränkungen unterliegen.	01. September 2022
Ankündigungen von Security Hub abonnieren	Sie können jetzt Security Hub-Ankündigungen mit Amazon Simple Notification Service (Amazon SNS) abonnieren, um Benachrichtigungen über Security Hub zu erhalten.	2p. August 2022
Regionserweiterung für regionsübergreifende Aggregation	Die regionsübergreifende Aggregation ist jetzt für Ergebnisse, Aktualisierungen und Einblicke in alle Regionen verfügbar. AWS GovCloud (US)	02.August 2022

Neue Produktintegrationen von Drittanbietern	Fortinet — FortiCNP ist eine Drittanbieter-Integration, die Security Hub-Ergebnisse empfängt, und JFrog ist eine Drittanbieter-Integration, die Ergebnisse an Security Hub sendet.	26. Juli 2022
EC2.27 ist eingestellt	Security Hub hat EC2.27 eingestellt — Beim Ausführen von EC2-Instances sollten keine Schlüsselpaare verwendet werden, eine frühere Kontrolle im Standard AWS Foundational Security Best Practices (FSBP).	20. Juli 2022
Lambda.2 unterstützt Python3.6 nicht mehr	Security Hub unterstützt Python3.6 nicht mehr als Parameter für Lambda.2 — Lambda-Funktionen sollten unterstützte Laufzeiten verwenden, eine Steuerung im Standard AWS Foundatio nal Security Best Practices (FSBP).	19. Juli 2022
AWS Security Hub fügt neue Sicherheitskontrollen hinzu	Neue Security Hub-Steue relemente sind für Kunden verfügbar, die den FSBP-Standard aktiviert haben. Für einige Kontrollen gelten regionale Einschränkungen.	22. Juni 2022

AWS Security Hub unterstützt eine neue Region	Security Hub ist jetzt im asiatisch-pazifischen Raum (Jakarta) verfügbar. Einige Steuerelemente sind in dieser Region nicht verfügbar.	7. Juni 2022
Verbesserte Integration zwischen AWS Security Hub und AWS Config	Security Hub-Benutzer können die Ergebnisse der AWS Config Regelauswertungen als Ergebnisse in Security Hub sehen.	6. Juni 2022
Es wurde die Möglichkeit hinzugefügt, automatisch aktivierte Standards zu deaktivieren	Für Benutzer, die mit integriert sind AWS Organizations, können Sie sich mit dieser Funktion beim Security Hub-Administratorkonto anmelden und neue Mitgliedskonten von den automatisch aktivierten Standards abmelden.	25. April 2022
Erweiterte regionsübergreifende Aggregation	Es wurde eine regionsübergreifende Aggregation hinzugefügt, um Status und Sicherheitsbewertungen zu kontrollieren.	20. April 2022
CompanyName und ProductName sind jetzt Attribute der obersten Ebene	Es wurden neue Attribute der obersten Ebene hinzugefügt, um Firmen- und Produktnamen für benutzerdefinierte Integrationen festzulegen	1. April 2022
Dem Standard „Best Practices für AWS grundlegende Sicherheit“ wurden neue Kontrollen hinzugefügt	Der Standard „Best Practices “ von AWS Foundational Security wurde um 5 neue Kontrollen erweitert.	31. März 2022

ASFF wurde um neue Objekte mit Ressourcendetails erweitert	`AwsRdsDbSecurityGroup` Ressourcentyp zu ASFF hinzugefügt.	25. März 2022
Zusätzliche Ressourcendetails in ASFF hinzugefügt	Zusätzliche Details zu `AwsAutoScalingScalingGroup` , `AwsElbLoadBalancer` `AwsRedshiftCluster` , und `AwsCodeBuildProject` hinzugefügt.	25. März 2022
Dem Standard „Bewährte Methoden für AWS grundlegende Sicherheit“ wurden neue Steuerelemente hinzugefügt	Der Standard „Best Practices “ von AWS Foundational Security wurde um 15 neue Kontrollen erweitert.	16. März 2022
Dem AWS Foundational Security Best Practices-Standard und dem Payment Card Industry Data Security Standard (PCI DSS) wurden neue Kontrollen hinzugefügt	Neue Steuerelemente für Amazon OpenSearch Service, Amazon RDS, Amazon EC2, Elastic Load Balancing und CloudFront zum Standard „Best Practices für AWS grundlegende Sicherheit“ hinzugefügt. Außerdem wurden dem PCI DSS zwei neue Steuerungen für OpenSearch Service hinzugefügt.	15. Februar 2022
ASFF wurde ein neues Feld hinzugefügt	Neues Feld hinzugefügt: Beispiel.	26. Januar 2022
Integration mit hinzugefügt AWS Health	AWS Health verwendet service-to-service Ereignisnachrichten, um Ergebnisse an Security Hub zu senden.	19. Januar 2022

Integration mit hinzugefügt AWS Trusted Advisor	Trusted Advisor sendet die Ergebnisse seiner Prüfungen als Security Hub-Ergebnisse an Security Hub. Security Hub sendet die Ergebnisse seiner AWS Foundational Security Best Practices-Prüfungen an Trusted Advisor.	18. Januar 2022
Objekte mit Ressourcendetails in ASFF wurden aktualisiert	`MixedInstancesPolicy` und `AvailabilityZones` wurden zu `AwsAutoScalingAutoScalingGroup` hinzugefügt. `MetadataOptions` wurde `AwsAutoScalingLaunchConfiguration` hinzugefügt. `BucketVersioningConfiguration` wurde `AwsS3Bucket` hinzugefügt.	20. Dezember 2021
Die Ausgabe für die ASFF-Dokumentation wurde aktualisiert	Die Beschreibungen der ASFF-Attribute waren zuvor in einem einzigen Thema zusammengefasst. Jedes Objekt der obersten Ebene und jedes Objekt mit Ressourcendetails befindet sich jetzt in einem eigenen Thema. Das Thema ASFF-Syntax enthält Links zu diesen Themen.	20. Dezember 2021

ASFF wurde um neue Objekte mit Ressourcendetails erweitert für AWS Network Firewall	For AWS Network Firewall hat die folgenden Objekte mit Ressourcendetails hinzugefügt: `AwsNetworkFirewallFirewall` `AwsNetworkFireFirewallPolicy`, und `AwsNetworkFirewallRuleGroup`.	20. Dezember 2021
Unterstützung für die neue Version von Amazon Inspector hinzugefügt	Security Hub ist in die neue Version von Amazon Inspector sowie in Amazon Inspector Classic integriert. Amazon Inspector sendet Ergebnisse an Security Hub.	29. November 2021
Der Schweregrad von EC2.19 wurde geändert	Der Schweregrad von EC2.19 (Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen) wurde von Hoch auf Kritisch geändert.	17. November 2021
Neue Integration mit Sonrai Dig	Security Hub bietet jetzt eine Integration mitSonrai Dig. Sonrai Digüberwacht Cloud-Umgebungen, um Sicherheitsrisiken zu identifizieren. Sonrai Digsendet Ergebnisse an Security Hub.	12. November 2021

Die Prüfung auf CIS CloudTrail 2.1- und 7.1-Steuerelemente wurde aktualisiert	CIS 2.1 und CloudTrail .1 überprüfen jetzt nicht nur, ob mindestens ein CloudTrail Multi-Region-Trail vorhanden ist, sondern überprüfen nun auch, ob der `ExcludeManagementEventSources` Parameter in mindestens einem der CloudTrail Multi-Region-Wanderwege leer ist.	9. November 2021
Unterstützung für VPC-Endpunkte hinzugefügt	Security Hub ist jetzt in VPC-Endpunkte integriert AWS PrivateLink und unterstützt diese.	3. November 2021
Dem Standard „Best Practices für AWS grundlegende Sicherheit“ wurden zusätzliche Kontrollen hinzugefügt	Neue Steuerelemente für Elastic Load Balancing (ELB.2 und ELB.8) und AWS Systems Manager (SSM.4) hinzugefügt.	2. November 2021
Dem Check für das EC2.19-Steuerelement wurden Ports hinzugefügt	EC2.19 prüft jetzt auch, ob Sicherheitsgruppen keinen uneingeschränkten Eingangszugriff auf die folgenden Ports zulassen: 3000 (Go, Node.js und Ruby Web Development Frameworks), 5000 (Python Web Development Frameworks), 8088 (Legacy-HTTP-Port) und 8888 (alternativer HTTP-Port)	27. Oktober 2021

Die Integration mit Logz.io Cloud SIEM wurde hinzugefügt	Logz.io ist ein Anbieter von Cloud-SIEM, der eine erweiterte Korrelation von Protokoll- und Ereignisdaten ermöglicht, um Sicherheitsteams dabei zu unterstützen, Sicherheitsbedrohungen in Echtzeit zu erkennen, zu analysieren und darauf zu reagieren. Logz.io erhält Ergebnisse von Security Hub.	25. Oktober 2021
Unterstützung für die regionsübergreifende Aggregation von Ergebnissen hinzugefügt	Durch die regionsübergreifende Aggregation können Sie sich alle Ihre Ergebnisse ansehen, ohne die Regionen ändern zu müssen. Administratorkonten wählen eine Aggregationsregion und verknüpfte Regionen aus. Die Ergebnisse für das Administratorkonto und seine Mitgliedskonten werden von den verknüpften Regionen zur Aggregationsregion zusammengefasst.	20. Oktober 2021

Objekte mit Ressourcendetails in ASFF wurden aktualisiert	Details zum Viewer-Zertifikat wurden hinzugefügt. `AwsCloudFrontDistribution` Zusätzliche Details wurden hinzugefügt `AwsCodeBuildProject` . Load Balancer-Attribute wurden hinzugefügt zu `AwsElbV2LoadBalancer` . Die Konto-ID des S3-Bucket-Besitzers wurde hinzugefügt. `AwsS3Bucket`	8. Oktober 2021
Neue Objekte mit Ressourcendetails zu ASFF hinzugefügt	ASFF wurde um die folgenden neuen Objekte mit Ressourcendetails erweitert :`AwsEc2VpcEndpointService` ,,`AwsEcrRepository` ,`AwsEksCluster` ,`AwsOpenSearchServiceDomain` , `AwsWafRateBasedRule` `AwsWafRegionalRateBasedRule` `AwsXrayEncryptionConfig`	8. Oktober 2021
Veraltete Runtime aus dem Lambda.2-Steuerelement entfernt	Im Standard „Best Practices für AWS grundlegende Sicherheit“ wurde die `dotnetcore2.1` Laufzeit aus [Lambda.2] entfernt. Lambda-Funktionen sollten unterstützte Laufzeiten verwenden.	6. Oktober 2021

Neuer Name für die Check Point-Integration	Die Integration mit Check Point Dome9 Arc heißt jetzt Check Point CloudGuard Posture Management. Der Integrations-ARN hat sich nicht geändert.	1. Oktober 2021
Die Integration mit Alcide wurde entfernt	Die Integration mit Alcide KAudit wurde eingestellt.	30. September 2021
Der Schweregrad von EC2.19 wurde geändert	Der Schweregrad von [EC2.19] Sicherheitsgruppen sollten keinen uneingesc hränkten Zugriff auf Ports mit hohem Risiko zulassen, wurde von Mittel auf Hoch geändert.	30. September 2021
Die Integration mit AWS Organizations wird jetzt in den Regionen Chinas unterstützt	Die Security Hub Hub-Integ ration mit Organizations wird jetzt in China (Peking) und China (Ningxia) unterstützt.	20. September 2021
Neue AWS Config Regel für die Steuerungen S3.1 und PCI.S3.6	Sowohl S3.1 als auch PCI.S3.6 stellen sicher, dass die Amazon S3 S3-Einstellung Block Public Access aktiviert ist. Die AWS Config Regel für diese Steuerelemente wurde von auf geändert. `s3-accoun t-level-public-acc ess-blocks` `s3-accoun t-level-public-acc ess-blocks-periodic`	14. September 2021

Veraltete Laufzeiten wurden aus dem Lambda.2-Steuerelement entfernt	Im Standard „Best Practices für AWS grundlegende Sicherheit“ wurden die `ruby2.5` Laufzeiten `nodejs10.x` und aus [Lambda.2] entfernt. Lambda-Funktionen sollten unterstützte Laufzeiten verwenden.	13. September 2021
Der Schweregrad der CIS 2.2-Steuerung wurde geändert	Im Benchmark-Standard der CIS AWS Foundations ist dies der Schweregrad für 2.2. — Stellen CloudTrail Sie sicher, dass die Validierung der Protokolldatei von Niedrig auf Mittel aktiviert ist.	13. September 2021
ECS.1, Lambda.2 und SSM.1 wurden im Standard „Best Practices für grundlegende Sicherheit“ aktualisiert AWS	Im Standard AWS Foundational Security Best Practices hat ECS.1 jetzt einen Parameter, der auf gesetzt ist. `SkipInactiveTaskDefinitions` `true` Dadurch wird sichergestellt, dass das Steuerelement nur aktive Aufgabendefinitionen überprüft. Für Lambda.2 wurde Python 3.9 zur Liste der Laufzeiten hinzugefügt. SSM.1 überprüft jetzt sowohl gestoppte als auch laufende Instanzen.	7. September 2021

Die PCI.Lambda.2-Steuerung schließt jetzt Lambda @Edge -Ressourcen aus	Im Payment Card Industry Data Security Standard (PCI DSS) -Standard schließt die PCI.Lambda.2-Steuerung nun Lambda @Edge -Ressourcen aus.	7. September 2021
Die Integration mit wurde hinzugefügt HackerOne Vulnerability Intelligence	Security Hub bietet jetzt eine Integration mitHackerOne Vulnerability Intelligence. Die Integration sendet die Ergebnisse an Security Hub.	7. September 2021
Objekte mit Ressourcendetails in ASFF wurden aktualisiert	Für`AwsKmsKey` , hinzugefügt`KeyRotationStatus` . Für`AwsS3Bucket` , hinzugefügt `AccessControlList` `BucketLoggingConfiguration` ,`BucketNotificationConfiguration` , und`BucketWebsiteConfiguration` .	2. September 2021
Neue Objekte mit Ressourcendetails zu ASFF hinzugefügt	ASFF wurden die folgenden neuen Ressourcendetailobjekte hinzugefügt: `AwsAutoScalingLaunchConfiguration` `AwsEc2VpnConnection` , und. `AwsEcrContainerImage`	2. September 2021
Dem `Vulnerabilities` Objekt in ASFF wurden Details hinzugefügt	In`Cvss`, hinzugefügt `Adjustments` und`Source`. `VulnerablePackages` In wurden der Dateipfad und der Paketmanager hinzugefügt.	2. September 2021

Systems Manager Explorer und OpsCenter Integration werden jetzt in den Regionen Chinas unterstützt	Die Security Hub Hub-Integration mit SSM Explorer OpsCenter wird jetzt in China (Peking) und China (Ningxia) unterstützt.	31. August 2021
Lambda.4-Steuerung außer Betrieb nehmen	Security Hub stellt die Steuerung ein [Lambda.4] Für Lambda-Funktionen sollte eine Warteschlange für unzustellbare Briefe konfiguriert sein. Wenn ein Steuerelement außer Betrieb genommen wird, wird es nicht mehr auf der Konsole angezeigt, und Security Hub führt keine Prüfungen daran durch.	31. August 2021
Das PCI.EC2.3-Steuerelement wird außer Betrieb genommen	Security Hub stellt die Steuerung ein [PCI.EC2.3] Unbenutzte EC2-Sicherheitsgruppen sollten entfernt werden. Wenn ein Steuerelement außer Betrieb genommen wird, wird es nicht mehr auf der Konsole angezeigt, und Security Hub führt keine Prüfungen daran durch.	27. August 2021
Ändern Sie die Art und Weise, wie Security Hub Ergebnisse an benutzerdefinierte Aktionen sendet	Wenn Sie Ergebnisse an eine benutzerdefinierte Aktion senden, sendet Security Hub jetzt jedes Ergebnis in einem separaten Security Hub Findings - Custom ActionEreignis.	20. August 2021

Es wurde ein neuer Code zur Begründung des Compliance-Status für benutzerdefinierte Lambda-Laufzeiten hinzugefügt	Ein neuer Code für die Gründe für den `LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE` Compliance-Status wurde hinzugefügt. Dieser Ursachencode weist darauf hin, dass Security Hub keine Prüfung anhand einer benutzerdefinierten Lambda-Laufzeit durchführen konnte.	20. August 2021
AWS Firewall Manager Die Integration wird jetzt in den Regionen Chinas unterstützt	Die Security Hub Hub-Integration mit Firewall Manager wird jetzt in China (Peking) und China (Ningxia) unterstützt.	19. August 2021
Neue Integrationen mit und Caveonix CloudForcepoint Cloud Security Gateway	Security Hub bietet jetzt Integrationen mit Caveonix Cloud undForcepoint Cloud Security Gateway. Beide Integrationen senden Ergebnisse an Security Hub.	10. August 2021

Neue `Region` Attribute `CompanyName` `ProductName` , und wurden zu ASFF hinzugefügt	`Region`Felder `CompanyName` `ProductName` , und wurden zur obersten Ebene der ASFF hinzugefügt. Diese Felder werden automatisch ausgefüllt und können, mit Ausnahme von benutzerdefinierten Produktintegrationen, nicht mit `BatchImportFindings` oder aktualisiert werden. `BatchUpdateFindings` Auf der Konsole werden beim Suchen nach Filtern diese neuen Felder verwendet. In der API verwenden die `ProductName` Filter `CompanyName` und die Attribute, die sich unter befinden`ProductFields` .	23. Juli 2021
Objekte mit Ressourcendetails in ASFF hinzugefügt und aktualisiert	Ein neuer `AwsRdsEventSubscription` Ressourcentyp und Ressourcendetails wurden hinzugefügt. Ressourcendetails für den `AwsEcsService` Ressourcentyp hinzugefügt. Dem Objekt mit den `AwsElasticsearchDomain` Ressourcendetails wurden Attribute hinzugefügt.	23. Juli 2021

Dem Standard „Best Practices für AWS grundlegende Sicherheit“ wurden Kontrollen hinzugefügt	Neue Steuerelemente für Amazon API Gateway (ApiGateway.5), Amazon EC2 (EC2.19), Amazon ECS (ECS.2), Elastic Load Balancing (ELB.7), Amazon OpenSearch Service (ES.5 bis ES.8), Amazon RDS (RDS.16 bis RDS.23), Amazon Redshift (Redshift.4) und Amazon SQS (SQS.1) hinzugefügt.	20. Juli 2021
Eine Berechtigung wurde innerhalb der mit dem Dienst verknüpften, rollenverwalteten Richtlinie verschoben	Die `config:PutEvaluations` Berechtigung wurde innerhalb der verwalteten Richtlinie verschoben `AWSSecurityHubServiceRolePolicy`, sodass sie auf alle Ressourcen angewendet wird.	14. Juli 2021
Dem Standard „Bewährte Methoden für AWS grundlegende Sicherheit“ wurden Kontrollen hinzugefügt	Neue Steuerelemente für Amazon API Gateway (ApiGateway.4), Amazon CloudFront (CloudFront.5 und CloudFront .6), Amazon EC2 CloudFront (EC2.17 und EC2.18), Amazon ECS (ECS.1), Amazon OpenSearch Service (ES.4), (IAM.21), Amazon RDS (RDS.15) und Amazon S3 AWS Identity and Access Management (S3.8) hinzugefügt.	8. Juli 2021

Es wurden neue Begründungscodes für den Compliance-Status für Kontrollergebnisse hinzugefügt	`INTERNAL_SERVICE_ERROR` weist darauf hin, dass ein unbekannter Fehler aufgetreten ist. `SNS_TOPIC_CROSS_ACCOUNT` gibt an, dass das SNS-Thema einem anderen Konto gehört. `SNS_TOPIC_INVALID` gibt an, dass das zugehörige SNS-Thema ungültig ist.	6. Juli 2021
Die Integration mit wurde hinzugefügt AWS Chatbot	Die Integration mit wurde hinzugefügt AWS Chatbot. Security Hub sendet Ergebnisse an AWS Chatbot.	30. Juni 2021
Der Richtlinie für die Verwaltung von dienstbezogenen Rollen wurde eine neue Berechtigung hinzugefügt	Der verwalteten Richtlinie wurde eine neue Berechtigung hinzugefügt`AWSSecurityHubServiceRolePolicy` , damit die dienstbezogene Rolle Bewertungsergebnisse liefern kann. AWS Config	29. Juni 2021
Neue und aktualisierte Objekte mit Ressourcendetails im ASFF	Neue Ressourcendetailobjekte für ECS-Cluster und ECS-Aufgabendefinitionen hinzugefügt. Das EC2-Instance-Objekt wurde aktualisiert und listet nun die zugehörigen Netzwerkschnittstellen auf. Die Client-Zertifikat-ID für die API Gateway V2-Stufen wurde hinzugefügt. Die Lebenszykluskonfiguration für S3-Buckets wurde hinzugefügt.	24. Juni 2021

Die Berechnung der aggregierten Kontrollstatus und der Standardsicherheitsbewertungen wurde aktualisiert	Security Hub berechnet jetzt alle 24 Stunden den Gesamtkontrollstatus und die Standardsicherheitsbewertung. Bei Administratorkonten spiegelt die Bewertung nun wider, ob die einzelnen Kontrollen für jedes Konto aktiviert oder deaktiviert sind.	23. Juni 2021
Aktualisierte Informationen zum Umgang mit gesperrten Konten durch Security Hub	Es wurden Informationen darüber hinzugefügt, wie Security Hub mit gesperrten Konten umgeht AWS.	23. Juni 2021
Es wurden Tabs hinzugefügt, um die aktivierten und deaktivierten Steuerelemente für das einzelne Administratorkonto anzuzeigen	Für das Administratorkonto enthalten die Hauptregister auf der Standarddetailseite aggregierte Informationen für alle Konten. Auf den neuen Registerkarten Aktiviert für dieses Konto und Deaktiviert für dieses Konto werden die Konten aufgeführt, die für das einzelne Administratorkonto aktiviert oder deaktiviert sind.	23. Juni 2021
Zu `java8.al2` den Parametern hinzugefügt für `Lambda.2`	Im Standard AWS Foundational Security Best Practices `java8.al2` zu den unterstützten Laufzeiten für das `Lambda.2` Steuerelement hinzugefügt.	8. Juni 2021

Neue Integrationen mit MicroFocus ArcSight und NETSCOUT Cyber Investigator	Integrationen mit MicroFocus ArcSight und NETSCOUT Cyber Investigator hinzugefügt. MicroFocus ArcSight erhält Ergebnisse von Security Hub. NETSCOUT Cyber Investigator sendet Ergebnisse an Security Hub.	7. Juni 2021
Details hinzugefügt für `AWSSecurityHubServiceRolePolicy`	Der Abschnitt „Verwaltete Richtlinien“ wurde aktualisiert, um Details für die bestehende verwaltete Richtlinie hinzuzufügen `AWSSecurityHubServiceRolePolicy`, die von der serviceverknüpften Security Hub Hub-Rolle verwendet wird.	4. Juni 2021
Neue Integration mit Jira Service Management	Der AWS Service Management Connector für Jira sendet Ergebnisse an Jira und verwendet sie, um Jira-Probleme zu erstellen. Wenn die Jira-Probleme aktualisiert werden, werden auch die entsprechenden Ergebnisse in Security Hub aktualisiert.	26. Mai 2021
Die Liste der unterstützten Kontrollen für die Region Asien-Pazifik (Osaka) wurde aktualisiert	Der Standard der CIS AWS Foundations und der Payment Card Industry Data Security Standard (PCI DSS) wurden aktualisiert und geben nun an, welche Kontrollen im asiatisch-pazifischen Raum (Osaka) nicht unterstützt werden.	21. Mai 2021

Neue Integration mit Sysdig Secure für die Cloud	Es wurde eine Integration mit Sysdig Secure für die Cloud hinzugefügt. Die Integration sendet die Ergebnisse an Security Hub.	14. Mai 2021
Dem Standard „Best Practices für AWS grundlegende Sicherheit“ wurden Kontrollen hinzugefügt	Neue Steuerelemente für Amazon API Gateway (ApiGateway.2 und ApiGateway.3), (CloudTrail.4 und CloudTrail .5), Amazon EC2 AWS CloudTrail (EC2.15 und EC2.16), (ElasticBeanstalk.1 und ElasticBeanstalk .2), (Lambda.4), Amazon RDS AWS Elastic Beanstalk (RDS.12 — RDS.14), Amazon Redshift AWS Lambda (Redshift.7), (.3 und .4) und (WAF.1) hinzugefügt. AWS Secrets Manager SecretsManager SecretsManager SecretsManager AWS WAF	10. Mai 2021
Aktualisierungen GuardDuty und Amazon RDS-Steuerelemente	Der Schweregrad wurde von `GuardDuty.1` und `PCI.GuardDuty.1` von Mittel auf Hoch geändert. Es wurde ein `databaseEngines` Parameter zu hinzugefügt`RDS.8`.	4. Mai 2021

Dem ASFF wurden neue Ressourcendetails hinzugefügt	In `Resources.Details` wurden neue Ressource ndetailobjekte für Amazon EC2-Netzwerk-ACLs, Amazon EC2-Subnetze und Umgebungen hinzugefügt. AWS Elastic Beanstalk	3. Mai 2021
Konsolenfelder hinzugefügt, um Filterwerte für EventBridge Amazon-Regeln bereitzustellen	Die neuen vordefinierten Filtermuster für Security Hub EventBridge Hub-Regeln bieten Konsolenfelder, mit denen Sie Filterwerte angeben können.	30. April 2021
Die Integration mit AWS Systems Manager Explorer wurde hinzugefügt und OpsCenter	Security Hub unterstützt jetzt eine Integration mit Systems Manager Explorer und OpsCenter. Die Integration erhält Ergebnisse von Security Hub und aktualisiert diese Ergebnisse in Security Hub.	26. April 2021
Neuer Typ für Produktintegrationen	Ein neuer Integrationstyp,`UPDATE_FINDINGS_IN_SECURITY_HUB` , weist darauf hin, dass eine Produktintegration die Ergebnisse aktualisiert, die sie von Security Hub erhält.	22. April 2021
„Hauptkonto“ wurde in „Administratorkonto“ geändert.	Der Begriff „Hauptkonto“ wird in „Administratorkonto“ geändert. Der Begriff wurde auch in der Security Hub Hub-Konsole und der API geändert.	22. April 2021

APIGateway.1 wurde aktualisiert, um HTTP durch Websocket zu ersetzen	Titel, Beschreibung und Problembehebung für ApiGateway.1 wurden aktualisiert. Das Steuerelement sucht nun nach der Protokollierung der Websocket-API-Ausführung statt nach der Protokollierung der HTTP-API-Ausführung.	9. April 2021
GuardDuty Die Amazon-Integration wird jetzt in Peking und Ningxia unterstützt	Die Security Hub Hub-Integration mit GuardDuty wird jetzt in den Regionen China (Peking) und China (Ningxia) unterstützt.	05. April 2021
`nodejs14.x` Zu den unterstützten Laufzeiten für die Lambda.2-Steuerung hinzugefügt	Das Lambda.2-Steuerelement im Standard Foundation Security Best Practices unterstützt jetzt die Laufzeit. `nodejs14.x`	30. März 2021
Security Hub im asiatisch-pazifischen Raum (Osaka) eröffnet	Security Hub ist jetzt in der Region Asien-Pazifik (Osaka) verfügbar.	29. März 2021
Zu den Suchdetails wurden Felder für die Suche nach Anbietern hinzugefügt	Im Bereich „Ergebnisdetails“ enthält der neue Abschnitt „Felder für die Suche nach Anbietern“ die Werte für Zuverlässigkeit, Kritikalität, verwandte Ergebnisse, Schweregrad und Typen.	24. März 2021

Option hinzugefügt, um sensible Ergebnisse von Amazon Macie zu erhalten	Die Integration mit Macie kann jetzt so konfiguriert werden, dass sensible Ergebnisse an Security Hub gesendet werden.	23. März 2021
Übergang AWS Organizations zur Kontoverwaltung	Für Kunden, die bereits über ein Administratorkonto mit Mitgliedskonten verfügen, wurden neue Informationen hinzugefügt, wie sie von der Verwaltung von Konten auf Einladung zur Verwaltung von Konten mithilfe von Organizations wechseln können.	22. März 2021
Neue Objekte in ASFF für Informationen zur Konfiguration von Amazon S3 Public Access Block	In `Resources` bietet ein neues Objekt mit `AwsS3AccountPublicAccessBlock` Ressourcentyp und Details Informationen zur Amazon S3 Public Access Block-Konfiguration für Konten. Im Objekt mit den `AwsS3Bucket` Ressourcendetails stellt das `PublicAccessBlockConfiguration` Objekt die Public Access Block-Konfiguration für den S3-Bucket bereit.	18. März 2021

Neues Objekt in ASFF, mit dem Anbieter gefunden werden können, um bestimmte Felder zu aktualisieren	Das neue `FindingProviderFields` Objekt in ASFF wird verwendet, `BatchImportFindings` um Werte für `Confidence` ,, `Criticality` `RelatedFindings` `Severity`, und bereitzustellen. `Types` Die ursprünglichen Felder sollten nur mit `BatchUpdateFindings` aktualisiert werden.	18. März 2021
Neues `DataClassification` Objekt für Ressourcen in ASFF	Das neue `Resources.DataClassification` Objekt in ASFF wird verwendet, um Informationen über sensible Daten bereitzustellen, die auf der Ressource erkannt wurden.	18. März 2021
`CONFIG_RETURNS_NOT_APPLICABLE` Mehrwert der verfügbaren Compliance-Statuscodes	Für den `NOT_AVAILABLE` Konformitätsstatus wurde der Ursachencode entfernt `RESOURCE_NO_LONGER_EXISTS` und der Ursachencode hinzugefügt `CONFIG_RETURNS_NOT_APPLICABLE` .	16. März 2021

Neue verwaltete Richtlinie für die Integration mit AWS Organizations	Eine neue verwaltete Richtlinie,`AWSSecurityHubOrganizationsAccess` , gewährt den Organizations die Berechtigungen, die für das Organisationsverwaltungskonto und das delegierte Security Hub-Administratorkonto erforderlich sind.	15. März 2021
Informationen zu verwalteten Richtlinien und dienstbezogenen Rollen wurden in das Kapitel Sicherheit verschoben	Die Informationen zu verwalteten Richtlinien wurden überarbeitet und erweitert. Sowohl die Informationen zu verwalteten Richtlinien als auch die Informationen zu dienstbezogenen Rollen wurden in das Kapitel Sicherheit verschoben.	15. März 2021
Neue Integration mit DB SecureCloud	SecureCloudDB wurde zur Liste der Integrationen von Drittanbietern hinzugefügt. SecureCloudDB ist ein Cloud-natives Datenbanksicherheitstool, das einen umfassenden Überblick über interne und externe Sicherheitslage und -aktivitäten bietet. SecureCloudDB sendet Ergebnisse an Security Hub.	4. März 2021
Der Schweregrad der Kontrollen CIS 1.1 und CIS 3.1 — CIS 3.14 wurde überarbeitet	Der Schweregrad der Kontrollen CIS 1.1 und CIS 3.1 — CIS 3.14 wurde auf Niedrig geändert.	3. März 2021

Das Steuerelement RDS.11 wurde entfernt	Das RDS.11-Steuereleme nt wurde aus dem Standard „Bewährte Methoden für grundlegende Sicherheit“ entfernt.	3. März 2021
Die Integration für Turbot wurde aktualisiert	Die Turbot-Integration wurde aktualisiert, um sowohl Ergebnisse zu senden als auch zu empfangen.	26. Februar 2021
Dem Standard „Bewährte Methoden für grundlegende Sicherheit“ wurden zusätzliche Kontrollen hinzugefügt	Neue Steuerelemente für Amazon API Gateway (ApiGateway.1), Amazon EC2 (EC2.9 und EC2.10), Amazon Elastic File System (EFS.2), Amazon OpenSearch Service (ES.2 und ES.3), Elastic Load Balancing (ELB.6) und () (KMS.3) hinzugefügt. AWS Key Management Service AWS KMS	11. Februar 2021
`ProductArn` Optionaler Filter zur `DescribeProducts` API hinzugefügt	Die `DescribeProducts` API-Operation enthält jetzt einen optionalen `ProductArn` Parameter. Der `ProductArn` Parameter wird verwendet, um die spezifisc he Produktintegration zu identifizieren, für die Details zurückgegeben werden sollen.	3. Februar 2021
Neue Integration mit Antivirus für Amazon S3 von Cloud Storage Security	Die Integration mit Antivirus for Amazon S3 sendet die Ergebnisse der Virensuche als Ergebnisse an Security Hub.	27. Januar 2021

Das Verfahren zur Berechnung der Sicherheitsbewertung für Administratorkonten wurde aktualisiert	Für ein Administratorkonto verwendet Security Hub einen separaten Prozess zur Berechnung der Sicherheitsbewertung. Das neue Verfahren stellt sicher, dass die Bewertung Kontrollen beinhaltet, die für Mitgliedskonten aktiviert, für das Administratorkonto jedoch deaktiviert sind.	21. Januar 2021
Neue Felder und Objekte im ASFF	Es wurde ein neues `Action` Objekt hinzugefügt, um Aktionen zu verfolgen, die gegen eine Ressource aufgetreten sind. Dem `AwsEc2NetworkInterface` Objekt wurden Felder hinzugefügt, um DNS-Namen und IP-Adressen zu verfolgen. Den Ressourcendetails wurde ein neues `AwsSsmPatchCompliance` Objekt hinzugefügt.	21. Januar 2021

Dem Standard „Best Practices für grundlegende Sicherheit“ wurden Kontrollen hinzugefügt	Neue Steuerelemente für Amazon CloudFront (CloudFront.1 bis CloudFront .4), Amazon DynamoDB (DynamoDB.1 bis DynamoDB.3), Elastic Load Balancing (ELB.3 bis ELB.5), Amazon RDS (RDS.9 bis RDS.11), Amazon Redshift (Redshift.1 bis Redshift.3 und Redshift.6) und Amazon SNS (SNS.1) hinzugefügt.	15. Januar 2021
Der Workflow-Status wird basierend auf dem Datensatzstatus oder dem Compliance-Status zurückgesetzt	Security Hub setzt den Workflow-Status automatisch von `NOTIFIED` oder `RESOLVED` auf zurück, `NEW` wenn ein archiviertes Ergebnis aktiviert wird oder wenn sich der Compliance-Status eines Befundes von entweder `PASSED` auf`FAILED`,`WARNING`, oder `NOT_AVAILABLE` ändert. Diese Änderungen deuten darauf hin, dass zusätzliche Untersuchungen erforderlich sind.	7. Januar 2021
Es wurden `ProductFields` Informationen für Ergebnisse hinzugefügt, die auf Kontrollen basieren	Für Ergebnisse, die anhand von Kontrollen generiert wurden, wurden Informationen über den Inhalt des `ProductFields` Objekts im AWS Security Finding Format (ASFF) hinzugefügt.	29. Dezember 2020

Aktualisierungen der verwalteten Erkenntnisse	Der Titel von Insight 5 wurde geändert. Es wurde ein neuer Insight (32) hinzugefügt, der nach IAM-Benutzern mit verdächtigen Aktivitäten sucht.	22. Dezember 2020
Aktualisierungen der IAM.7- und Lambda.1-Steuerelemente	Im Standard AWS Foundational Security Best Practices wurden die Parameter für IAM.7 aktualisiert. Der Titel und die Beschreibung von Lambda.1 wurden aktualisiert.	22. Dezember 2020
Erweiterte Integration mit ITSM ServiceNow	Die ServiceNow ITSM-Integration ermöglicht es Benutzern, automatisch Vorfälle oder Probleme zu erstellen, wenn ein Security Hub Hub-Ergebnis eingeht. Aktualisierungen dieser Vorfälle oder Probleme führen zu Aktualisierungen der Ergebnisse in Security Hub.	11. Dezember 2020
Neue Integration mit AWS Audit Manager	Security Hub bietet jetzt eine Integration mit AWS Audit Manager. Die Integration ermöglicht es Audit Manager, kontrollbasierte Ergebnisse von Security Hub zu erhalten.	08. Dezember 2020
Neue Integration mit Aqua Security Kube-Bench	Security Hub hat eine Integration mit Aqua Security Kube-Bench hinzugefügt. Die Integration sendet die Ergebnisse an Security Hub.	24. November 2020

Cloud Custodian ist jetzt in den Regionen Chinas verfügbar	Die Integration mit Cloud Custodian ist jetzt in den Regionen China (Peking) und China (Ningxia) verfügbar.	24. November 2020
`BatchImportFindings` kann jetzt verwendet werden, um zusätzliche Felder zu aktualisieren	Bisher konnten Sie die `Types` Felder`Confidence`, `Criticality` `RelatedFindings` `Severity`, und nicht `BatchImportFindings` zum Aktualisieren verwenden. Wenn diese Felder nicht von aktualisiert wurden`BatchUpdateFindings`, können sie nun von aktualisiert werden`BatchImportFindings`. Sobald sie von aktualisiert wurden`BatchUpdateFindings`, können sie nicht mehr von aktualisiert werden`BatchImportFindings`.	24. November 2020

Security Hub ist jetzt integriert in AWS Organizations	Kunden können jetzt Mitglieds konten mithilfe ihrer Organisat ionskontokonfiguration verwalten. Das Organisat ionsverwaltungskonto bestimmt das Security Hub-Administratorkonto, das festlegt, welche Organisat ionskonten in Security Hub aktiviert werden sollen. Der manuelle Einladungsprozess kann weiterhin für Konten verwendet werden, die nicht Teil einer Organisation sind.	23. November 2020
Das separate Suchlistenformat für Steuerelemente mit hohem Volumen wurde entfernt	Die Ergebnisliste für ein Steuerelement verwendet nicht mehr das Seitenfor mat „Ergebnisse“, wenn es eine sehr große Anzahl von Ergebnissen gibt.	19. November 2020
Neue und aktualisierte Integrationen von Drittanbi etern	Security Hub unterstützt jetzt Integrationen mit cloudtame r.io, 3CoreSec, Prowler und Kubernetes Security. StackRox IBM QRadar sendet keine Ergebnisse mehr. Es empfängt nur Ergebnisse.	30. Oktober 2020

Option zum Herunterladen der Ergebnisliste von der Seite mit den Kontrolldetails hinzugefügt.	Auf der Seite mit den Kontrolldetails gibt es eine neue Download-Option, mit der Sie die Ergebnisliste in eine CSV-Datei herunterladen können. Die heruntergeladene Liste berücksichtigt alle Filter, die in der Liste enthalten sind. Wenn Sie bestimmte Ergebnisse ausgewählt haben, enthält die heruntergeladene Liste nur diese Ergebnisse.	26. Oktober 2020
Option zum Herunterladen der Liste der Steuerelemente von der Standarddetailseite hinzugefügt.	Auf der Standarddetailseite können Sie mit einer neuen Download-Option die Kontrollliste in eine CSV-Datei herunterladen. Die heruntergeladene Liste berücksichtigt alle Filter, die in der Liste enthalten sind. Wenn Sie ein bestimmtes Steuerelement ausgewählt haben, enthält die heruntergeladene Liste nur dieses Steuerelement.	26. Oktober 2020

Neue und aktualisierte Partnerintegrationen	Security Hub ist jetzt in integriert ThreatModeler. Die folgenden Partnerintegrationen wurden aktualisiert, um ihren neuen Produktnamen Rechnung zu tragen. Twistlock Enterprise Edition heißt jetzt Palo Alto Networks - Prisma Cloud Compute. Demisto, ebenfalls von Palo Alto Networks, ist jetzt Cortex XSOAR und Redlock ist jetzt Prisma Cloud Enterprise.	23. Oktober 2020
Security Hub in China (Peking) und China (Ningxia) eröffnet	Security Hub ist jetzt in den Regionen China (Peking) und China (Ningxia) verfügbar.	21. Oktober 2020
Überarbeitetes Format für ASFF-Attribute und Integrationen von Drittanbietern	Die Listen der ASFF-Attribute und Partnerintegrationen verwenden jetzt ein listenbasiertes Format anstelle von Tabellen. Die ASFF-Syntax, die Attribute und die Taxonomie der Typen sind jetzt in separaten Themen zusammengefasst.	15. Oktober 2020
Die Standard-Detailseite wurde neu gestaltet	Auf der Standarddetailseite für einen aktivierten Standard wird jetzt eine Liste mit Steuerelementen im Registerformat angezeigt. Die Registerkarten filtern die Kontrollliste auf der Grundlage des Kontrollstatus.	7. Oktober 2020

CloudWatch Ereignisse wurden ersetzt durch EventBridge	Verweise auf Amazon CloudWatch Events wurden durch Amazon ersetzt EventBridge.	1. Oktober 2020
Neue Integrationen mit Blue Hexagon for AWS, Alcide KAudit und Palo Alto Networks VM-Series.	Security Hub ist jetzt in Blue Hexagon for AWS, Alcide KAudit und Palo Alto Networks VM-Series integriert. Blue Hexagon for AWS und KAudit senden Ergebnisse an Security Hub. VM-Series erhält Ergebnisse von Security Hub.	30. September 2020
Neue und aktualisierte Objekte mit Ressourcendetails in ASFF	Neue `Resources.Details` Objekte für`AwsApiGatewayRestApi` ,, `AwsApiGatewayStage` `AwsApiGatewayV2Api` ,`AwsApiGatewayV2Stage` , `AwsCertificateManagerCertificate` `AwsElbLoadBalancer` `AwsIamGroup` , und `AwsRedshiftCluster` hinzugefügt. Es wurden Details zu den `AwsIamAccessKey` Objekten`AwsCloudFrontDistribution` , `AwsIamRole` und hinzugefügt.	30. September 2020

Neues `ResourceRole` Attribut für Ressourcen in ASFF, um zu verfolgen, ob es sich bei einer Ressource um einen Akteur oder ein Ziel handelt.	Das `ResourceRole` Attribut für Ressourcen gibt an, ob die Ressource das Ziel der Suchaktivität oder der Täter der Findungsaktivität ist. Die gültigen Werte sind `ACTOR` und `TARGET`.	30. September 2020
AWS Systems Manager Patch Manager wurde zu den verfügbaren AWS Serviceintegrationen hinzugefügt	AWS Systems Manager Patch Manager ist jetzt in Security Hub integriert. Patch Manager sendet Ergebnisse an Security Hub, wenn Instances in der Flotte eines Kunden nicht mehr dem Patch-Compliance-Standard entsprechen.	22. September 2020
Der Standard „Bewährte Methoden für AWS grundlegende Sicherheitslösungen“ wurde um neue Kontrollen erweitert	Neue Steuerungen für die folgenden Dienste hinzugefügt: Amazon EC2 (EC2.7 und EC2.8), Amazon EMR (EMR.1), IAM (IAM.8), Amazon RDS (RDS.4 bis RDS.8), Amazon S3 (S3.6) und (.1 und .2). AWS Secrets Manager SecretsManager SecretsManager	15. September 2020
Neue Kontextschlüssel `BatchUpdateFindings` für die IAM-Richtlinie zur Steuerung des Zugriffs auf Felder	IAM-Richtlinien können jetzt so konfiguriert werden, dass der Zugriff auf Felder und Feldwerte bei der Verwendung eingeschränkt wird. `BatchUpdateFindings`	10. September 2020

Erweiterter Zugriff auf `BatchUpdateFindings` für Mitgliedskonten	Standardmäßig haben Mitgliedskonten jetzt denselben Zugriff `BatchUpdateFindings` wie Administratorkonten.	10. September 2020
Neue Kontrollen AWS KMS im Foundational Security Best Practices Standard	Zwei neue Kontrollen (KMS.1 und KMS.2) wurden dem Foundational Security Best Practices Standard hinzugefügt. Die neuen Kontrollen prüfen, ob IAM-Richtlinien den Zugriff auf Entschlüsselungsaktionen einschränken. AWS KMS	9. September 2020
Die Ergebnisse für Kontrollen auf Kontoebene wurden entfernt	Security Hub generiert keine Ergebnisse mehr auf Kontoebene für eine Kontrolle. Es werden nur Ergebnisse auf Ressourcenebene generiert.	1. September 2020
Neues PatchSummary Objekt in ASFF	Das `PatchSummary` Objekt wurde der ASFF hinzugefügt. Das `PatchSummary` Objekt stellt Informationen zur Patch-Konformität einer Ressource im Verhältnis zu einem ausgewählten Konformitätsstandard bereit.	1. September 2020

Die Seite mit den Kontrolldetails wurde neu gestaltet	Die Detailseite für Steuerelemente wurde neu gestaltet. Die Liste mit den Ergebnissen von Kontrollen enthält Registerkarten, mit denen Sie die Liste schnell nach dem Konformitätsstatus filtern können. Sie können auch schnell unterdrückte Ergebnisse einsehen. Jeder Eintrag bietet Zugriff auf zusätzliche Details zur Suchressource, zur AWS Config Suchregel und zu Suchnotizen.	28. August 2020
Neue Filteroptionen für Ergebnisse	Für die Suche nach Filtern können Sie den Filter ist nicht verwenden, um Ergebnisse zu finden, bei denen ein Feldwert nicht dem Filterwert entspricht. Sie können den Befehl „Beginnt nicht mit“ verwenden, um nach Ergebnissen zu suchen, bei denen ein Feldwert nicht mit dem angegebenen Filterwert beginnt.	28. August 2020

Neue Objekte mit Ressourcendetails in ASFF	Es wurden neue `Resources.Details` Objekte für die folgenden Ressourcentypen hinzugefügt: `AwsDynamoDbTable` `AwsEc2Eip` `AwsIamPolicy` ,,`AwsIamUser` ,`AwsRdsDbCluster` ,`AwsRdsDbClusterSnapshot` , `AwsRdsDbSnapshot` `AwsSecretsManagerSecret`	18. August 2020
Neue Integration mit RSA Archer	Security Hub ist jetzt in RSA Archer integriert. RSA Archer erhält Ergebnisse von Security Hub.	18. August 2020
Neues Beschreibungsfeld für AwsKmsKey	Dem `AwsKmsKey` Objekt unter wurde ein `Description` Feld hinzugefügt `Resources.Details` .	18. August 2020
Felder wurden hinzugefügt zu AwsRdsDbInstance	Dem `AwsRdsDbInstance` Objekt unter wurden mehrere Attribute hinzugefügt `Resources.Details` .	18. August 2020

Die Art und Weise, wie Security Hub den Gesamtstatus einer Kontrolle bestimmt, wurde aktualisiert	Bei Kontrollen, für die keine Ergebnisse vorliegen, lautet der Status Keine Daten statt Unbekannt. Der Kontrollstatus umfasst sowohl Ergebnisse auf Konto- als auch auf Ressourcenebene. Der Kontrollstatus verwendet nicht den Workflow-Status von Ergebnissen, es sei denn, unterdrückte Ergebnisse werden ignoriert.	13. August 2020
Die Art und Weise, wie Security Hub die Sicherheitsbewertung für einen Standard berechnet, wurde aktualisiert	Bei der Berechnung der Sicherheitsbewertung für einen Standard ignoriert Security Hub jetzt Steuerelemente mit dem Status Keine Daten. Die Sicherheitsbewertung ist das Verhältnis der bestandenen Kontrollen zu den aktivierten Kontrollen, ausgenommen Kontrollen ohne Daten.	13. August 2020
Neue Option zur automatischen Aktivierung neuer Kontrollen in aktivierten Standards	Es wurde eine Einstellungsoption hinzugefügt, um neue Steuerelemente in aktivierten Standards automatisch zu aktivieren. Sie können diese Option auch mithilfe der `UpdateSecurityHubConfiguration` API-Operation konfigurieren.	31. Juli 2020

Neue Kontrollen für den Payment Card Industry Data Security Standard (PCI DSS) - Standard	Dem PCI DSS-Standard wurden neue Steuerungen hinzugefügt. Die Kennungen der neuen Steuerelemente lauten PCI.DMS.1, PCI.EC2.5 , PCI.EC2.6, PCI.ELBV2.1, PCI. GuardDuty.1, PCI.IAM.7 , PCI.IAM.8, PCI.S3.5, PCI.S3.6, PCI. SageMaker.1, PCI.SSM.2 und PCI.SSM.3.	29. Juli 2020
Neue und aktualisierte Kontrollen für den Standard Foundational Security Best Practices	Dem Standard „Best Practices “ von Foundational Security wurden neue Kontrollen hinzugefügt. Die Kennungen der neuen Kontrollen lauten AutoScaling .1, DMS.1, EC2.4, EC2.6, S3.5 und SSM.3. Der Titel von ACM.1 wurde aktualisiert und der Wert des Parameters wurde auf 30 geändert. `daysToExp iration`	29. Juli 2020
Neues `Vulnerabilities` Objekt in der ASFF	Das `Vulnerabilities` Objekt wurde hinzugefügt, das Informationen über Sicherhei tslücken bereitstellt, die mit dem Befund in Verbindung stehen.	1. Juli 2020
Neue `Resource.Details` Objekte im ASFF für Auto Scaling Scaling-Gruppen, EC2-Volumes und EC2-VPCs	Die Objekte`AwsAutoSc alingAutoScalingGr oup` , und `AWSEc2Vol ume` wurden hinzugefügt. `AwsEc2Vpc` `Resource. Details`	1. Juli 2020

Neues `NetworkPath` Objekt in der ASFF	Das `NetworkPath` Objekt wurde hinzugefügt, das Informationen über einen Netzwerkpfad bereitstellt, der mit dem Ergebnis zusammenhängt.	1. Juli 2020
Ergebnisse automatisch auflösen, `Compliance.Status` wenn `PASSED`	Falls dies der Fall `Compliance.Status` ist`PASSED`, setzt Security Hub bei Ergebnissen aus Kontrollen automatisch `Workflow.Status` auf`RESOLVED`.	24. Juni 2020
AWS Command Line Interface Beispiele	AWS CLI Syntax und Beispiele für mehrere Security Hub Hub-Aufgaben hinzugefügt. Beinhaltet die Aktivierung von Security Hub, die Verwaltung von Erkenntnissen, die Verwaltung von Standards und Kontrollen, die Verwaltung von Produktintegrationen und die Deaktivierung von Security Hub.	24. Juni 2020
Neues `Severity.Original` Attribut im ASFF	Das Attribut `Severity.Original` wurde hinzugefügt, wobei es sich um den ursprünglichen Schweregrad des Ergebnisanbieters handelt. Dies ersetzt das veraltete `Severity.Product` -Attribut.	20. Mai 2020

Neues `Compliance.StatusReasons` Objekt im ASFF für Details zum Status eines Steuerelements	Es wurde das Objekt `Compliance.StatusReasons` hinzugefügt, das zusätzlichen Kontext für den aktuellen Status einer Kontrolle bereitstellt.	20. Mai 2020
Neuer AWS grundlegender Standard für bewährte Sicherheitsverfahren	Der neue Standard „Bewährte Methoden für AWS grundlegende Sicherheitsverfahren“ wurde hinzugefügt. Dabei handelt es sich um eine Reihe von Kontrollen, die erkennen, wann Ihre bereitgestellten Konten und Ressourcen von den bewährten Sicherheitsmethoden abweichen.	22. April 2020
Neue Konsolenoption zum Aktualisieren des Workflow-Status für ein Ergebnis	Es wurden Informationen zur Verwendung der Security Hub-Konsole oder -API hinzugefügt, um den Workflow-Status für Ergebnisse festzulegen.	16. April 2020
Neue `BatchUpdateFindings` API für Kundenaktualisierungen von Ergebnissen	Es wurden Informationen zur Verwendung von `BatchUpdateFindings` hinzugefügt, um Informationen im Zusammenhang mit dem Prozess der Untersuchung eines Ergebnisses zu aktualisieren. `BatchUpdateFindings` ersetzt `UpdateFindings`, das veraltet ist.	16. April 2020

Aktualisierungen des AWS Security Finding Format (ASFF)	Mehrere neue Ressourcentypen hinzugefügt. Dem `Severity`-Objekt wurde ein neues `Label`-Attribut hinzugefügt. `Label` soll das `Normalized` -Feld ersetzen. Es wurde ein neues `Workflow`-Objekt hinzugefügt, um den Prozess einer Untersuchung zu einem Ergebnis zu verfolgen . `Workflow` enthält ein `Status`-Attribut, das das vorhandene `Workflows tate` -Attribut ersetzt.	12. März 2020
Aktualisierungen der Seite „Integrationen“	Aktualisiert, um die Änderungen an der Integrationsseite anzuzeigen. Für jede Integration zeigt die Seite nun die Integrationskategorie und ob jede Integration Ergebnisse an Security Hub sendet oder Ergebnisse von Security Hub empfängt. Sie enthält auch die spezifischen Schritte, die erforderlich sind, um jede Integration zu ermöglichen.	26. Februar 2020

Neue Produktintegrationen von Drittanbietern	Die folgenden neuen Produktintegrationen wurden hinzugefügt: Cloud Custodian, FireEye Helix, Forcepoint CASB, Forcepoint DLP, Forcepoint NGFW, Rackspace Cloud Native Security und Vectra.ai Cognito Detect.	21. Februar 2020
Neuer Sicherheitsstandard für den Payment Card Industry Data Security Standard (PCI DSS)	Der Security Hub-Sicherheitsstandard für den Payment Card Industry Data Security Standard (PCI DSS) wurde hinzugefügt. Wenn dieser Standard aktiviert ist, führt Security Hub automatisierte Prüfungen anhand von Kontrollen durch, die sich auf die PCI DSS-Anforderungen beziehen.	13. Februar 2020
Aktualisierungen des AWS Security Finding Format (ASFF)	Ein Feld für zugehörige Anforderungen für Standardkontrollen wurde hinzugefügt. Neue Ressourcentypen und neue Ressourcendetails wurden hinzugefügt. Mit dem ASFF können Sie jetzt bis zu 32 Ressourcen bereitstellen.	5. Februar 2020
Neue Option zum Deaktivieren einzelner Sicherheitsstandardkontrollen	Es wurden Informationen hinzugefügt, wie Sie steuern können, ob jedes einzelne Sicherheitsstandard-Steuerelement aktiviert ist.	15. Januar 2020

Aktualisierungen der Terminologie und Konzepte	Einige Beschreibungen wurden aktualisiert und Terminologie und Konzepten wurde mit neuen Begriffen ergänzt.	21. September 2019
AWS Version für allgemeine Verfügbarkeit von Security Hub	Inhaltsaktualisierungen, um den Verbesserungen Rechnung zu tragen, die in der Vorschauphase an Security Hub vorgenommen wurden.	25. Juni 2019
Es wurden Schritte zur Problembehebung für CIS AWS Foundations-Prüfungen hinzugefügt	Es wurden Korrekturschritte zu den in Security Hub unterstützten AWS Sicherheitsstandards hinzugefügt.	15. April 2019
Vorschauversion von AWS Security Hub	Die Vorabversion des AWS Security Hub Hub-Benutzerhandbuchs wurde veröffentlicht.	18. November 2018

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.