



Leitfaden zur Implementierung

Automatisierte Sicherheitsreaktion auf AWS



Automatisierte Sicherheitsreaktion auf AWS: Leitfaden zur Implementierung

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Marken, die nicht im Besitz von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Übersicht über die Lösung	1
Features und Vorteile	3
Anwendungsfälle	4
Konzepte und Definitionen	5
Übersicht über die Architektur	7
Architekturdiagramm	7
AWSÜberlegungen zu Well-Architected Design	9
Operative Exzellenz	9
Sicherheit	9
Zuverlässigkeit	10
Leistungseffizienz	10
Kostenoptimierung	10
Nachhaltigkeit	10
Einzelheiten zur Architektur	11
AWS Security Hub Integration	11
Kontoübergreifende Problembehebung	11
Spielbücher	12
Zentralisierte Protokollierung	12
Benachrichtigungen	13
AWS-Dienste in dieser Lösung	13
Planen Sie Ihren Einsatz	15
Kosten	15
Beispiel für eine Kostentabelle	15
Preisbeispiele (monatlich)	20
Zusätzliche Kosten für optionale Funktionen	25
Sicherheit	27
IAM-Rollen	27
Unterstützt AWS-Regionen	28
Kontingente	29
Kontingente für AWS Dienste in dieser Lösung	29
AWS CloudFormation Kontingente	30
Amazon EventBridge regelt Kontingente	30
AWS-Bereitstellung von Security Hub	30
Stapel im Vergleich StackSets zur Bereitstellung	30

Stellen Sie die Lösung bereit	32
Entscheiden, wo jeder Stack eingesetzt werden soll	32
Entscheiden Sie, wie die einzelnen Stacks bereitgestellt werden	34
Konsolidierte Kontrollergebnisse	34
AWS CloudFormation Vorlagen	35
Unterstützung für Admin-Konten	35
Mitgliedskonten	36
Rollen der Mitglieder	37
Integration des Ticketsystems	37
Automatisierte Bereitstellung - StackSets	37
Voraussetzungen	38
Überblick über die Bereitstellung	38
(Optional) Schritt 0: Starten Sie einen Ticketsystem-Integrationsstapel	40
Schritt 1: Starten Sie den Admin-Stack im delegierten Security Hub-Administratorkonto	43
Schritt 2: Installieren Sie die Behebungsrollen in jedem AWS Security Hub-Mitgliedskonto	44
Schritt 3: Starten Sie den Member-Stack für jedes AWS Security Hub-Mitgliedskonto und jede Region	45
Automatisierte Bereitstellung — Stacks	46
Voraussetzungen	46
Überblick über die Bereitstellung	46
(Optional) Schritt 0: Starten Sie einen Ticketsystem-Integrationsstapel	47
Schritt 1: Starten Sie den Admin-Stack	50
Schritt 2: Installieren Sie die Behebungsrollen in jedem AWS Security Hub-Mitgliedskonto	55
Schritt 3: Starten Sie den Member-Stack	57
Schritt 4: (Optional) Passen Sie die verfügbaren Abhilfemaßnahmen an	61
Überwachen Sie die Lösung mit Service Catalog AppRegistry	63
Verwenden Sie CloudWatch Application Insights	64
Bestätigen Sie die mit der Lösung verknüpften Kostenangaben	65
Aktivieren Sie die mit der Lösung verknüpften Kostenzuweisungs-Tags	66
AWS Cost Explorer	66
Überwachen Sie den Betrieb der Lösung mit einem CloudWatch Amazon-Dashboard	67
Aktivierung von CloudWatch Metriken, Alarmen und Dashboards	67
Verwenden des CloudWatch Dashboards	68
Änderung der Alarmschwellen	69
Alarmbenachrichtigungen abonnieren	72
Aktualisieren Sie die Lösung	73

Aktualisierung von Versionen vor v1.4	73
Aktualisierung von v1.4 und höher	73
Aktualisierung von v2.0.x	73
Fehlerbehebung	74
Lösungsprotokolle	74
Lösung eines bekannten Problems	75
Probleme mit bestimmten Abhilfemaßnahmen	78
PutS3 schlägt fehl BucketPolicyDeny	79
Wie deaktiviere ich die Lösung	79
Kontakt Support	80
Fall erstellen	80
Wie können wir helfen?	80
Zusätzliche Informationen	80
Helfen Sie uns, Ihren Fall schneller zu lösen	81
Löse jetzt oder kontaktiere uns	81
Deinstallieren Sie die Lösung	82
V1.0.0-V1.2.1	82
V1.3.x	82
V1.4.0 und später	83
Leitfaden für Administratoren	84
Teile der Lösung aktivieren und deaktivieren	84
SNSBeispielbenachrichtigungen	85
Benutze die Lösung	88
Erste Schritte mit Automated Security Response on AWS	88
Bereite die Konten vor	88
AWSConfig aktivieren	89
Aktivieren Sie den AWS Sicherheitshub	89
Ermöglichen Sie konsolidierte Kontrollergebnisse	90
Konfigurieren Sie die regionsübergreifende Suchaggregation	91
Benennen Sie ein Security Hub-Administratorkonto	91
Erstellen Sie die Rollen für selbstverwaltete Berechtigungen StackSets	92
Erstellen Sie die unsicheren Ressourcen, die zu Beispielergebnissen führen	93
Erstellen Sie CloudWatch Protokollgruppen für verwandte Steuerelemente	94
Stellen Sie die Lösung für Tutorial-Konten bereit	95
Stellen Sie den Admin-Stack bereit	95
Stellen Sie den Mitglieds-Stack bereit	96

Stellen Sie den Mitgliederrollen-Stack bereit	97
Abonnieren Sie das Thema SNS	97
Korrigieren Sie die Ergebnisse der Beispiele	98
Initiieren Sie die Behebung	98
Vergewissern Sie sich, dass das Problem durch die Behebung behoben wurde	99
Verfolgen Sie die Ausführung der Behebung	99
EventBridge Regel	99
Ausführung von Step Functions	99
SSM-Automatisierung	100
CloudWatch Gruppe protokollieren	100
Ermöglichen Sie vollautomatische Problembehebungen	100
Vergewissern Sie sich, dass Sie über keine Ressourcen verfügen, auf die diese Feststellung möglicherweise versehentlich angewendet wird	100
Aktivieren Sie die Regel	101
Konfigurieren Sie die Ressource	101
Vergewissern Sie sich, dass das Problem durch die Behebung behoben wurde	99
Bereinigen	102
Löschen Sie die Beispielressourcen	102
Löschen Sie den Admin-Stack	103
Löschen Sie den Mitglieds-Stack	103
Löschen Sie den Stapel der Mitgliedsrollen	103
Löschen Sie die beibehaltenen Rollen	104
Planen Sie, dass die gespeicherten KMS Schlüssel gelöscht werden	104
Löschen Sie die Stacks für selbstverwaltete Berechtigungen StackSets	105
Entwicklerhandbuch	107
Quellcode	107
Spielbücher	107
Neue Abhilfemaßnahmen hinzufügen	176
Übersicht	177
Schritt 1. Erstellen Sie ein Runbook in dem/den Mitgliedskonto (en)	177
Schritt 2. Erstellen Sie eine IAM Rolle in dem/den Mitgliedskonto (en)	178
Schritt 3: (Optional) Erstellen Sie eine automatische Behebungsregel im Administratorkonto	178
Ein neues Playbook hinzufügen	178
AWS Systems Manager Parameterspeicher	179
SNSThema — Fortschritt der Problembehebung	180

Ein SNS Themenabonnement filtern	180
SNSAmazon-Thema — CloudWatch Alarme	181
Runbook bei Konfigurationsergebnissen starten	182
Referenz	183
Anonymisierte Datenerhebung	183
Zugehörige Ressourcen	184
Mitwirkende	185
Überarbeitungen	186
Hinweise	192
.....	cxciii

Automatischer Umgang mit Sicherheitsbedrohungen mit vordefinierten Reaktions- und Abhilfemaßnahmen in AWS Security Hub

Veröffentlichungsdatum: August 2020 ([letzte Aktualisierung](#): Dezember 2024)

Dieser Implementierungsleitfaden bietet einen Überblick über die Automated Security AWS Response-Lösung, ihre Referenzarchitektur und ihre Komponenten, Überlegungen zur Planung der Bereitstellung sowie Konfigurationsschritte für die Bereitstellung der Automated Security AWS Response-On-Lösung in der Amazon Web Services (AWS) Cloud.

Verwenden Sie diese Navigationstabelle, um schnell Antworten auf diese Fragen zu finden:

Wenn du willst.	Lesen.
Informieren Sie sich über die Kosten für den Betrieb dieser Lösung	Kosten
Machen Sie sich mit den Sicherheitsüberlegungen für diese Lösung vertraut	Sicherheit
Erfahren Sie, wie Sie Kontingente für diese Lösung einplanen	Kontingente
Erfahren Sie, welche AWS Regionen für diese Lösung unterstützt werden	Unterstützte AWS Regionen
Sehen Sie sich die in dieser Lösung enthaltene AWS CloudFormation Vorlage an oder laden Sie sie herunter, um die Infrastrukturressourcen (den „Stack“) für diese Lösung automatisch bereitzustellen	AWS CloudFormation - Vorlagen
Greifen Sie auf den Quellcode zu und verwenden Sie optional das AWS Cloud Development Kit (AWSCDK), um die Lösung bereitzustellen.	GitHub Repository

Die kontinuierliche Weiterentwicklung der Sicherheit erfordert proaktive Maßnahmen zur Sicherung von Daten, was es für Sicherheitsteams schwierig, teuer und zeitaufwändig machen kann, zu reagieren. Die AWS Lösung Automated Security Response on hilft Ihnen, schnell auf

Sicherheitsprobleme zu reagieren, indem sie vordefinierte Antworten und Abhilfemaßnahmen bereitstellt, die auf branchenüblichen Compliance-Standards und bewährten Verfahren basieren.

[Automated Security Response on AWS ist eine AWS Lösung, mit AWS Security Hubder Sie Ihre Sicherheit verbessern und Ihre Workloads an den Best Practices für Well-Architected Security ausrichten können \(SEC10\)](#). Diese Lösung erleichtert es AWS Security Hub Kunden, häufig auftretende Sicherheitslücken zu beheben und ihren Sicherheitsstatus zu verbessern. AWS

Sie können bestimmte Playbooks auswählen, die in Ihrem Security Hub-Primärkonto bereitgestellt werden sollen. Jedes Playbook enthält die erforderlichen benutzerdefinierten Aktionen, [Identity and Access Management Zugriffsmanagement-Rollen](#) (IAM), [EventBridge Amazon-Regeln](#), [AWS Systems Manager Manager-Automatisierungsdokumente](#) und [AWS Lambda](#)Funktionen, die [AWS Step Functions](#)erforderlich sind, um einen Korrektur-Workflow innerhalb eines einzelnen AWS Kontos oder mehrerer Konten zu starten. Abhilfemaßnahmen werden über das Aktionsmenü ausgeführt AWS Security Hub und ermöglichen es autorisierten Benutzern, einen Fehler in all ihren AWS Security Hub verwalteten Konten mit einer einzigen Aktion zu korrigieren. Sie können beispielsweise Empfehlungen des Center for Internet Security (CIS) AWS Foundations Benchmark, einem Compliance-Standard für die Sicherung von AWS Ressourcen, anwenden, um sicherzustellen, dass Kennwörter innerhalb von 90 Tagen ablaufen, und die Verschlüsselung der darin gespeicherten Ereignisprotokolle durchzusetzen. AWS

Note

Die Problembehebung ist für Notfälle vorgesehen, die sofortiges Handeln erfordern. Bei dieser Lösung werden nur dann Änderungen zur Behebung von Ergebnissen vorgenommen, wenn diese von Ihnen über die AWS Security Hub Management-Konsole initiiert wurden oder wenn die automatische Problembehebung mithilfe der EventBridge Amazon-Regel für eine bestimmte Kontrolle aktiviert wurde. Um diese Änderungen rückgängig zu machen, müssen Sie die Ressourcen manuell in ihren ursprünglichen Zustand zurückversetzen.

Beachten Sie bei der Korrektur von AWS Ressourcen, die als Teil des CloudFormation Stacks bereitgestellt werden, dass dies zu Abweichungen führen kann. Wenn möglich, korrigieren Sie die Stack-Ressourcen, indem Sie den Code, der die Stack-Ressourcen definiert, ändern und den Stack aktualisieren. Weitere Informationen finden Sie unter [Was ist Drift?](#) im AWS CloudFormation Benutzerhandbuch.

Automated Security Response on AWS umfasst das Playbook zur Behebung der Sicherheitsstandards, die im Rahmen der folgenden Maßnahmen definiert wurden:

- [Benchmark v1.2.0 für AWS Grundlagen des Center for Internet Security \(CIS\)](#)
- [CISAWSBenchmark für Grundlagen v1.4.0](#)
- [CISAWSBenchmark für Stiftungen v3.0.0](#)
- [AWSBewährte Methoden für grundlegende Sicherheit \(\) v.1.0.0 FSBP](#)
- [Datensicherheitsstandard der Zahlungskartenbranche \(PCI-\) v3.2.1 DSS](#)
- [Nationales Institut für Standards und Technologie \(NIST\) SP 800-53 Rev. 5](#)

Die Lösung umfasst auch ein Security Controls (SC) -Playbook für die [Funktion „Konsolidierte Kontrollergebnisse“](#) von AWS Security Hub. Weitere Informationen finden Sie unter [Playbooks](#).

In diesem Implementierungsleitfaden werden architektonische Überlegungen und Konfigurationsschritte für die Bereitstellung von Automated Security Response auf AWS einer Lösung in der AWS Cloud erörtert. Er enthält Links zu [AWS CloudFormation](#) Vorlagen, mit denen die für die Implementierung dieser Lösung erforderlichen AWS Rechen-, Netzwerk-, Speicher- und anderen Dienste gestartet, konfiguriert und ausgeführt werdenAWS, wobei AWS bewährte Methoden für Sicherheit und Verfügbarkeit verwendet werden.

Der Leitfaden richtet sich an IT-Infrastrukturarchitekten, Administratoren und DevOps Fachleute, die über praktische Erfahrung mit der Architektur in der AWS Cloud verfügen.

Features und Vorteile

Automated Security Response on AWS bietet die folgenden Funktionen:

Automatisches Korrigieren von Ergebnissen bei bestimmten Kontrollen

Aktivieren Sie EventBridge Amazon-Regeln für Kontrollen, um Ergebnisse für diese Kontrolle automatisch zu korrigieren, sobald sie im AWS Security Hub angezeigt werden.

Verwalten Sie Problembehebungen für mehrere Konten und Regionen von einem Standort aus

Initiieren Sie von einem AWS Security Hub-Administratorkonto aus, das als Aggregationsziel für die Konten und Regionen Ihrer Organisation konfiguriert ist, eine Behebung eines Fehlers in einem beliebigen Konto und jeder Region, in der die Lösung bereitgestellt wird.

Lassen Sie sich über Abhilfemaßnahmen und Ergebnisse benachrichtigen

Abonnieren Sie das von der Lösung bereitgestellte SNS Amazon-Thema, um benachrichtigt zu werden, wenn Abhilfemaßnahmen eingeleitet werden und ob die Behebung erfolgreich war oder nicht.

Integrieren Sie in Ticketsysteme wie Jira oder ServiceNow

Damit Ihr Unternehmen auf Abhilfemaßnahmen reagieren kann (z. B. die Aktualisierung Ihres Infrastrukturcodes), kann diese Lösung Tickets an Ihr externes Ticketsystem weiterleiten.

Verwendung AWSConfigRemediations in den Partitionen GovCloud und China

Bei einigen der in der Lösung enthaltenen Abhilfemaßnahmen handelt es sich um Neupakete AWS eigener AWSConfigRemediation Dokumente, die in der kommerziellen Partition verfügbar sind, jedoch nicht in oder in GovCloud China. Stellen Sie diese Lösung bereit, um diese Dokumente in diesen Partitionen zu verwenden.

Erweitern Sie die Lösung um benutzerdefinierte Problembehebungs- und Playbook-Implementierungen

Die Lösung ist so konzipiert, dass sie erweiterbar und anpassbar ist. Um eine alternative Problembehebungsimplementierung zu spezifizieren, stellen Sie maßgeschneiderte AWS Systems Manager Manager-Automatisierungsdokumente und AWS IAM -Rollen bereit. Stellen Sie ein benutzerdefiniertes Playbook bereit, um eine ganze Reihe neuer Steuerelemente zu unterstützen, die in der Lösung nicht implementiert sind.

Anwendungsfälle

Erzwingen Sie die Einhaltung eines Standards in allen Konten und Regionen Ihres Unternehmens

Stellen Sie das Playbook für einen Standard bereit (z. B. AWS Foundational Security Best Practices), um die bereitgestellten Abhilfemaßnahmen nutzen zu können. Initiieren Sie automatisch oder manuell Abhilfemaßnahmen für Ressourcen in allen Konten und Regionen, in denen die Lösung eingesetzt wird, um Ressourcen zu reparieren, die nicht den Richtlinien entsprechen.

Stellen Sie benutzerdefinierte Abhilfemaßnahmen oder Playbooks bereit, um die Compliance-Anforderungen Ihres Unternehmens zu erfüllen

Verwenden Sie die bereitgestellten Orchestrator-Komponenten als Framework. Erstellen Sie benutzerdefinierte Problembehebungen, um out-of-compliance Ressourcen entsprechend den spezifischen Anforderungen Ihres Unternehmens zu adressieren.

Konzepte und Definitionen

In diesem Abschnitt werden die wichtigsten Konzepte beschrieben und die für diese Lösung spezifische Terminologie definiert:

Anwendung

Eine logische Gruppe von AWS Ressourcen, die Sie als Einheit betreiben möchten.

Problembhebung, Runbook zur Problembhebung

Eine Implementierung einer Reihe von Schritten zur Behebung eines Fehlers. Beispielsweise würde eine Korrektur für das Steuerelement Security Control (SC) Lambda.1 „Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten“ die Richtlinie der entsprechenden AWS Lambda-Funktion dahingehend ändern, dass Aussagen, die den öffentlichen Zugriff ermöglichen, entfernt werden.

Runbook steuern

Eines aus einer Reihe von AWS Systems Manager (SSM) -Automatisierungsdokumenten, die der Orchestrator verwendet, um eine eingeleitete Behebung für eine bestimmte Steuerung an das richtige Behebungs-Runbook weiterzuleiten. Beispielsweise werden die Behebungen für SC Lambda.1 und AWS Foundational Security Best Practices (FSBP) Lambda.1 mit demselben Behebungs-Runbook implementiert. Der Orchestrator ruft das Kontroll-Runbook für jedes Steuerelement mit den Namen `_Lambda.1` bzw. `-SC_2.0.0_Lambda.1` auf. ASR AFSBP ASR Jedes Kontroll-Runbook ruft dasselbe Behebungs-Runbook auf, das in diesem Fall - wäre. ASR RemoveLambdaPublicAccess

Orchestrator

Die von der Lösung bereitgestellten Step Functions, die als Eingabe ein Findobjekt von AWS Security Hub verwendet und das richtige Kontroll-Runbook im Zielkonto und in der Zielregion aufruft. Der Orchestrator benachrichtigt das SNS Lösungsthema außerdem, wenn die Wiederherstellung gestartet wird und wann die Wiederherstellung erfolgreich ist oder fehlschlägt.

Standard

Eine Gruppe von Kontrollen, die von einer Organisation als Teil eines Compliance-Frameworks definiert wurden. Einer der von AWS Security Hub und dieser Lösung unterstützten Standards ist beispielsweise AWSFSBP.

Steuerung

Eine Beschreibung der Eigenschaften, über die eine Ressource verfügen sollte oder nicht, um den Vorschriften zu entsprechen. Das Steuerelement AWS FSBP Lambda.1 besagt beispielsweise, dass AWS Lambda-Funktionen den öffentlichen Zugriff verbieten sollten. Eine Funktion, die öffentlichen Zugriff ermöglicht, würde diese Kontrolle nicht erfüllen.

konsolidierte Kontrollergebnisse, Sicherheitskontrolle, Ansicht der Sicherheitskontrollen

Eine Funktion von AWS Security Hub, die, wenn sie aktiviert ist, Ergebnisse mit ihrer konsolidierten Kontrolle anzeigt IDs, IDs anstatt solche, die einem bestimmten Standard entsprechen. Beispielsweise sind die Steuerelemente AWS FSBP S3.2, CIS v1.2.0 2.3, CIS v1.4.0 2.1.5.2 und PCI - DSS v3.2.1 S3.1 alle dem konsolidierten Steuerelement (SC) S3.2 „S3-Buckets sollten öffentlichen Lesezugriff verbieten“ zugeordnet. Wenn diese Funktion aktiviert ist, werden SC-Runbooks verwendet.

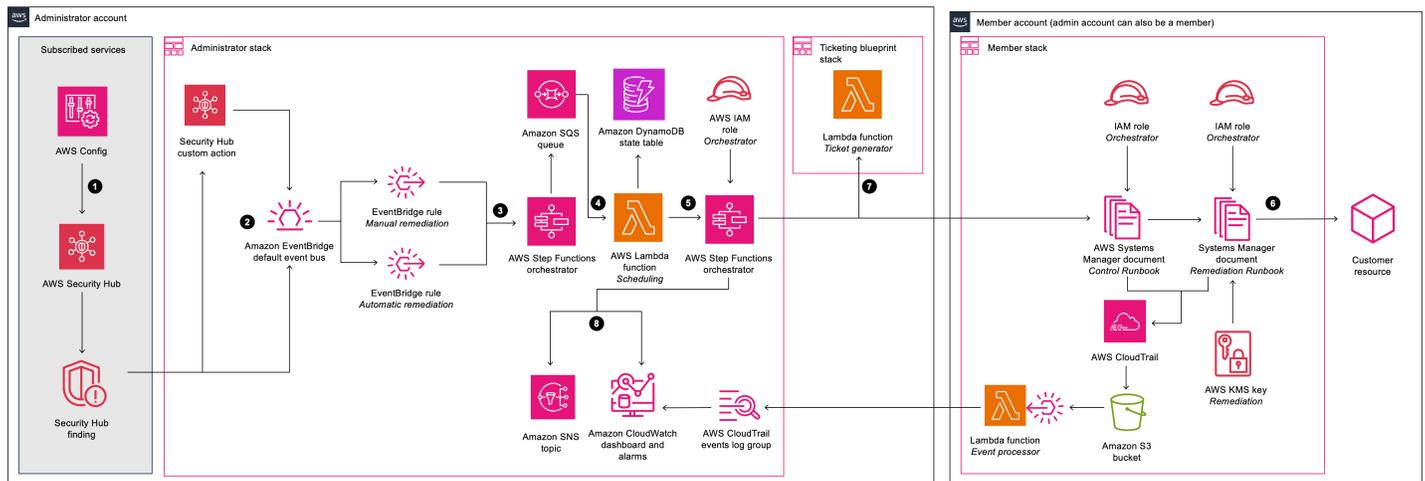
Eine allgemeine AWS Begriffsübersicht finden Sie im [AWS Glossar](#).

Übersicht über die Architektur

Dieser Abschnitt enthält ein Referenzdiagramm zur Implementierungsarchitektur für die mit dieser Lösung bereitgestellten Komponenten.

Architekturdiagramm

Durch die Bereitstellung dieser Lösung mit den Standardparametern wird die folgende Umgebung in der AWS Cloud erstellt.



Automatisierte Sicherheitsreaktion auf die AWS Architektur

Note

AWS CloudFormation Ressourcen werden aus AWS Cloud Development Kit (AWSCDK) - Konstrukten erstellt.

Der allgemeine Prozessablauf für die mit der AWS CloudFormation Vorlage bereitgestellten Lösungskomponenten sieht wie folgt aus:

1. Erkennen: [AWS Security Hub](#) bietet Kunden einen umfassenden Überblick über ihren AWS Sicherheitsstatus. Es hilft ihnen, ihre Umgebung anhand der Standards und bewährten Verfahren der Sicherheitsbranche zu messen. Es funktioniert, indem es Ereignisse und Daten von anderen AWS Diensten wie AWS Config, Amazon Guard Duty und AWS Firewall Manager sammelt. Diese Ereignisse und Daten werden anhand von Sicherheitsstandards wie CIS AWS Foundations

Benchmark analysiert. Ausnahmen werden als Ergebnisse in der AWS Security Hub Konsole bestätigt. Neue Ergebnisse werden als [EventBridgeAmazon-Events](#) gesendet.

2. Initiieren: Sie können mithilfe benutzerdefinierter Aktionen Ereignisse anhand von Ergebnissen einleiten, die zu EventBridge Ereignissen führen. AWS Security Hub [Mit benutzerdefinierten Aktionen](#) und EventBridge [Regeln](#) wird eine automatische Sicherheitsreaktion in AWS Playbooks ausgelöst, um auf die Ergebnisse zu reagieren. Die Lösung bietet:
 - a. Eine EventBridge Regel, die dem benutzerdefinierten Aktionsereignis entspricht
 - b. Eine EventBridge Ereignisregel für jedes unterstützte Steuerelement (standardmäßig deaktiviert), das dem Erkennungsereignis in Echtzeit entspricht

Sie können das Menü Benutzerdefinierte Aktionen in der Security Hub Hub-Konsole verwenden, um eine automatische Problembekämpfung einzuleiten. Nach sorgfältigen Tests in einer Umgebung außerhalb der Produktionsumgebung können Sie auch automatische Problembekämpfungen aktivieren. Sie können Automatisierungen für einzelne Bekämpfungen aktivieren — Sie müssen automatische Initiierungen nicht für alle Bekämpfungen aktivieren.

3. Vorabbehebung: Verarbeitet das Behebungsereignis im Administratorkonto und [AWS Step Functions](#) bereitet es für die Planung vor.
4. Zeitplan: Die Lösung ruft die [AWS Lambda](#) Planungsfunktion auf, um das Behebungsereignis in der [Amazon DynamoDB DynamoDB-Statustabelle](#) zu platzieren.
5. Orchestrieren: Im Administratorkonto verwendet Step Functions kontoübergreifende [AWS Identity and Access Management](#)(IAM) Rollen. Step Functions ruft die Problembekämpfung in dem Mitgliedskonto auf, das die Ressource enthält, die zu der Sicherheitslücke geführt hat.
6. Korrigieren: Ein [AWS Systems Manager Automatisierungsdokument](#) im Mitgliedskonto führt die Aktion durch, die zur Bekämpfung des Fehlers auf der Zielressource erforderlich ist, z. B. die Deaktivierung des öffentlichen Lambda-Zugriffs.

Optional können Sie die Aktionsprotokollfunktion in den Mitglieds-Stacks mit dem Parameter aktivieren. EnableCloudTrailForASRActionLog Diese Funktion erfasst die von der Lösung ausgeführten Aktionen in Ihren Mitgliedskonten und zeigt sie im [CloudWatchAmazon-Dashboard](#) der Lösung an.

7. (Optional) Erstellen Sie ein Ticket: Wenn Sie den TicketGenFunctionNameParameter verwenden, um das Ticketing im Admin-Stack zu aktivieren, ruft die Lösung die bereitgestellte Lambda-Funktion für den Ticketgenerator auf. Diese Lambda-Funktion erstellt ein Ticket in Ihrem Ticketservice, nachdem die Problembekämpfung im Mitgliedskonto erfolgreich ausgeführt wurde. Wir bieten [Stacks für die Integration](#) mit Jira und. ServiceNow

8. Benachrichtigen und protokollieren: Das Playbook protokolliert die Ergebnisse in einer CloudWatch [Protokollgruppe](#), sendet eine Benachrichtigung an ein [Amazon Simple Notification Service](#) (AmazonSNS) -Thema und aktualisiert den Security Hub Hub-Befund. Die Lösung führt in den [Ergebnisnotizen einen Prüfpfad der Aktionen](#).

AWSÜberlegungen zu Well-Architected Design

Diese Lösung wurde mit Best Practices aus dem AWS Well-Architected Framework entwickelt, das Kunden dabei unterstützt, zuverlässige, sichere, effiziente und kostengünstige Workloads in der Cloud zu entwerfen und zu betreiben. In diesem Abschnitt wird beschrieben, wie die Entwurfsprinzipien und Best Practices des Well-Architected Framework bei der Erstellung dieser Lösung angewendet wurden.

Operative Exzellenz

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren des Pfeilers [Operational](#) Excellence konzipiert haben.

- Ressourcen, die als IaC definiert sind und verwenden. CloudFormation
- Soweit möglich, wurden Abhilfemaßnahmen mit den folgenden Merkmalen durchgeführt:
 - Idempotenz
 - Fehlerbehandlung und Berichterstattung
 - Protokollierung
 - Wiederherstellung eines bekannten Zustands der Ressourcen bei einem Ausfall

Sicherheit

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren der [Sicherheitssäule](#) konzipiert haben.

- IAM wird für die Authentifizierung und Autorisierung verwendet.
- Der Umfang der Rollenberechtigungen sollte so eng wie möglich sein. In vielen Fällen erfordert diese Lösung jedoch Platzhalterberechtigungen, um auf beliebige Ressourcen zugreifen zu können.

Zuverlässigkeit

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren der Zuverlässigkeitskomponente konzipiert haben.

- Security Hub erstellt weiterhin Ergebnisse, wenn die zugrunde liegende Ursache des Fehlers durch die Behebung nicht behoben wird.
- Serverlose Dienste ermöglichen eine bedarfsgerechte Skalierung der Lösung.

Leistungseffizienz

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren des Pfeilers [Leistungseffizienz](#) konzipiert haben.

- Diese Lösung wurde als Plattform konzipiert, die Sie erweitern können, ohne Orchestrierung und Berechtigungen selbst implementieren zu müssen.

Kostenoptimierung

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren des Pfeilers [Kostenoptimierung](#) konzipiert haben.

- Serverlose Dienste ermöglichen es Ihnen, nur für das zu bezahlen, was Sie tatsächlich nutzen.
- Verwenden Sie das kostenlose Kontingent für die SSM Automatisierung in jedem Konto

Nachhaltigkeit

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren der [Säule Nachhaltigkeit](#) konzipiert haben.

- Serverlose Dienste ermöglichen es Ihnen, nach Bedarf nach oben oder unten zu skalieren.

Einzelheiten zur Architektur

In diesem Abschnitt werden die Komponenten und AWS Dienste, aus denen diese Lösung besteht, sowie die Architekturdetails zum Zusammenspiel dieser Komponenten beschrieben.

AWS Security Hub Integration

Durch die Bereitstellung des `aws-sharr-deploy` Stacks wird eine Integration mit der benutzerdefinierten Aktionsfunktion von AWS Security Hub erreicht. Wenn AWS Security Hub Konsolenbenutzer Findings for Remediation auswählen, leitet die Lösung den Ergebnisdatensatz zur Behebung mithilfe eines weiteren AWS Step Functions

Kontoübergreifende Berechtigungen und AWS Systems Manager Runbooks müssen mithilfe der Vorlagen und für alle AWS Security Hub Konten (Administrator und Mitglied) bereitgestellt werden. `aws-sharr-member.template` `aws-sharr-member-roles.template` CloudFormation [Weitere Informationen finden Sie unter Playbooks.](#) Diese Vorlage ermöglicht eine automatische Problembehebung im Zielkonto.

Benutzer können mithilfe der CloudWatch Amazon-Event-Regeln automatisch automatische Abhilfemaßnahmen pro Problembehebung einleiten. Diese Option aktiviert die vollautomatische Behebung von Ergebnissen, sobald sie gemeldet werden. AWS Security Hub Standardmäßig sind automatische Initiierungen deaktiviert. Diese Option kann jederzeit während oder nach der Installation des Playbooks geändert werden, indem die Regeln für CloudWatch Ereignisse im AWS Security Hub Administratorkonto aktiviert werden.

Kontoübergreifende Problembehebung

Automated Security Response on AWS verwendet kontoübergreifende Rollen, um mithilfe von kontoübergreifenden Rollen über primäre und sekundäre Konten hinweg zu arbeiten. Diese Rollen werden während der Installation der Lösung für Mitgliedskonten bereitgestellt. Jeder Problembehebung wird eine individuelle Rolle zugewiesen. Dem Behebungsprozess im primären Konto wird die Berechtigung erteilt, die Behebungsrolle in dem Konto zu übernehmen, für das eine Korrektur erforderlich ist. Die Wiederherstellung wird von AWS Systems Manager Manager-Runbooks durchgeführt, die in dem Konto ausgeführt werden, für das eine Wiederherstellung erforderlich ist.

Playbooks

Eine Reihe von Abhilfemaßnahmen ist in einem Paket zusammengefasst, das als Playbook bezeichnet wird. Playbooks werden mithilfe der Vorlagen dieser Lösung installiert, aktualisiert und entfernt. Informationen zu den in den einzelnen Playbooks unterstützten Problembehebungen finden Sie im [Entwicklerhandbuch](#) -> Playbooks. Diese Lösung unterstützt derzeit die folgenden Playbooks:

- Security Control, ein Playbook, das auf die Funktion Consolidated Control Findings von AWS Security Hub abgestimmt ist, wurde am 23. Februar 2023 veröffentlicht.

Important

Wenn [Consolidated Control Findings](#) in Security Hub aktiviert sind, ist dies das einzige Playbook, das in der Lösung aktiviert werden sollte.

- [Center for Internet Security \(CIS\) Benchmarks der Amazon Web Services Foundation, Version 1.2.0](#), veröffentlicht am 18. Mai 2018.
- [Center for Internet Security \(CIS\) Benchmarks der Amazon Web Services Foundation, Version 1.4.0](#), veröffentlicht am 9. November 2022.
- [Center for Internet Security \(CIS\) Benchmarks der Amazon Web Services Foundation, Version 3.0.0](#), veröffentlicht am 13. Mai 2024.
- [AWS Bewährte Methoden für grundlegende Sicherheit \(FSBP\) Version 1.0.0](#), veröffentlicht im März 2021.
- [Datensicherheitsstandards der Zahlungskartenbranche \(PCI-DSS\), Version 3.2.1](#), veröffentlicht im Mai 2018.
- [Version 5.0.0 des Nationalen Instituts für Standards und Technologie \(NIST\)](#), veröffentlicht im November 2023.

Zentralisierte Protokollierung

Automatisierte Sicherheitsreaktion auf AWS Protokolle an eine einzelne CloudWatch Protokollgruppe, SO0111-. SHARR Diese Protokolle enthalten eine detaillierte Protokollierung der Lösung zur Problembehandlung und Verwaltung der Lösung.

Benachrichtigungen

Diese Lösung verwendet ein Amazon Simple Notification Service (AmazonSNS) -Thema, um die Ergebnisse der Problembekämpfung zu veröffentlichen. Sie können Abonnements für dieses Thema verwenden, um die Funktionen der Lösung zu erweitern. Sie können beispielsweise E-Mail-Benachrichtigungen senden und Trouble-Tickets aktualisieren.

AWSDienste in dieser Lösung

Die Lösung verwendet die folgenden Dienste. Für die Nutzung der Lösung sind Kerndienste erforderlich, und unterstützende Dienste verbinden die Kerndienste.

AWS Dienst	Beschreibung
Amazon EventBridge	Kern. Stellt Ereignisse bereit, die die Orchestrator-Schrittfunktion auslösen, wenn ein Fehler behoben wird.
AWS IAM	Kern. Stellt viele Rollen bereit, um Problembekämpfungen auf verschiedenen Ressourcen zu ermöglichen.
AWS Lambda	Kern. Stellt mehrere Lambda-Funktionen bereit, die vom Step Function Orchestrator zur Behebung von Problemen verwendet werden.
AWS Security Hub	Kern. Bietet Kunden einen umfassenden Überblick über ihren AWS Sicherheitsstatus.
AWS Step Functions	Kern. Stellt einen Orchestrator bereit, der die Behebungsdokumente mit AWS Systems Manager Manager-Aufrufen aufruft. API
AWS Systems Manager	Kern. Stellt System Manager-Dokumente (Link zum Dokument) bereit, die die auszuführende Behebungslogik enthalten.
AWS CloudTrail	Unterstützend. Zeichnet Änderungen auf, die die Lösung an Ihren AWS Ressourcen

AWS Dienst	Beschreibung
	vornimmt, und zeigt sie auf einem CloudWatch Dashboard an.
<u>Amazon CloudWatch</u>	Unterstützend. Stellt Protokollgruppen bereit, die von den verschiedenen Playbooks zum Protokollieren der Ergebnisse verwendet werden. Sammelt Messwerte, die auf einem benutzerdefinierten Dashboard mit Alarmen angezeigt werden.
<u>AWS DynamoDB</u>	Unterstützend. Speichert die zuletzt ausgeführte Behebung in jedem Konto und jeder Region, um die Planung von Korrekturen zu optimieren.
<u>Service Catalog AppRegistry</u>	Unterstützend. Stellt eine Anwendung für bereitgestellte Stacks bereit, um Kosten und Nutzung zu verfolgen.
<u>Amazon Simple Notification Service</u>	Unterstützend. Stellt SNS Themen bereit, die eine Benachrichtigung erhalten, sobald eine Problembehebung abgeschlossen ist.
<u>AWS SQS</u>	Unterstützend. Hilft bei der Planung von Korrekturen, sodass die Lösung Korrekturen parallel ausführen kann.

Planen Sie Ihren Einsatz

In diesem Abschnitt werden die Kosten, die Netzwerksicherheit, der Support AWS-Regionen, die Kontingente und andere Überlegungen vor der Bereitstellung der Lösung beschrieben.

Kosten

Sie sind für die Kosten der AWS Dienste verantwortlich, die für den Betrieb dieser Lösung verwendet werden. Zum jetzigen Zeitpunkt belaufen sich die Kosten für den Betrieb dieser Lösung mit den Standardeinstellungen in den USA Ost (Nord-Virginia) AWS-Region auf etwa 21,17\$ für 300 Behebungen pro Monat, 134,86\$ für 3.000 Behebungen pro Monat und 1.281,01\$ für 30.000 Behebungen pro Monat. Die Preise sind freibleibend. Vollständige Informationen finden Sie auf der Seite AWS mit den Preisen für jeden Service, der in dieser Lösung genutzt wird.

Note

Viele AWS Services beinhalten ein kostenloses Kontingent — ein Basisangebot, das Kunden kostenlos nutzen können. Die tatsächlichen Kosten können über oder unter den angegebenen Preisbeispielen liegen.

Wir empfehlen, ein [Budget](#) zu erstellen AWS Cost Explorer, um die Kosten besser kontrollieren zu können. Die Preise sind freibleibend. Vollständige Informationen finden Sie auf der Preisseite der einzelnen in dieser Lösung verwendeten AWS Dienste.

Beispiel für eine Kostentabelle

Die Gesamtkosten für den Betrieb dieser Lösung hängen von den folgenden Faktoren ab:

- Die Anzahl der AWS Security Hub Mitgliedskonten
- Die Anzahl der aktiven, automatisch aufgerufenen Behebungen
- Die Häufigkeit der Problembhebung

Diese Lösung verwendet die folgenden AWS Komponenten, für die je nach Konfiguration Kosten anfallen. Preisbeispiele werden für kleine, mittlere und große Unternehmen bereitgestellt.

Service	Kostenloses Kontingent	Preisgestaltung [USD]
AWS Systems Manager Automation — Anzahl der Schritte	100.000 Schritte pro Konto und Monat	Über das kostenlose Kontingent hinaus wird jeder Basisschritt mit 0,002\$ pro Schritt berechnet. Bei Automatisierungen mit mehreren Konten werden alle Schritte, einschließlich der Schritte, die auf Konten von Kindern ausgeführt werden, nur für das ursprüngliche Konto gezählt.
AWS Systems Manager Automation — Schrittdauer	5.000 Sekunden pro Monat	Nach Ablauf des kostenlosen Kontingents von 5.000 Sekunden pro Monat werden für jeden executeScript aws:Action-Schritt 0,00003\$ pro Sekunde berechnet.
AWS Systems Manager Automation — Speicher	Kein kostenloses Kontingent	0,046\$ pro GB pro Monat
AWS Systems Manager Automation — Datenübertragung	Kein kostenloses Kontingent	0,900\$ pro übertragenem GB (für kontoübergreifendes Konto oder) out-of-Region
AWS Security Hub - Sicherheitsüberprüfungen	Kein kostenloses Kontingent	Die ersten 100.000 checks/account/Region/month kosten 0,0010 USD pro Scheck Die nächsten 400.000 checks/account/Region/month kosten 0,0008\$ pro Scheck

Service	Kostenloses Kontingent	Preisgestaltung [USD]
		Über 500.000 checks/account/Region/month kosten 0,0005\$ pro Scheck
AWS Security Hub - Auffinden von Verschluckungsereignissen	Die ersten 10.000 sind events/account/Region/month kostenlos. Suche nach Datenaufnahmeereignissen im Zusammenhang mit den Sicherheitsüberprüfungen von Security Hub.	Über 10.000\$ events/account/Region/month kosten 0,00003\$ pro Ereignis
Amazon CloudWatch — Metriken	Grundlegende Überwachungsmetriken (im Abstand von 5 Minuten) 10 detaillierte Überwachungsmetriken (im Intervall von 1 Minute) 1 Million API Anfragen (gilt nicht für GetMetricData und GetMetricWidgetImage)	<p>Die ersten 10.000 Metriken kosten 0,30\$ pro Metrik pro Monat</p> <p>Die nächsten 240.000 Metriken kosten 0,10\$ pro Metrik pro Monat</p> <p>Die nächsten 750.000 Metriken kosten 0,05\$ pro Metrik pro Monat</p> <p>Über 1.000.000 Metriken kosten 0,02\$ pro Metrik pro Monat</p> <p>APIAnrufe kosten 0,01\$ pro 1.000 Anfragen</p>
Amazon CloudWatch — Übersicht	3 Dashboards für bis zu 50 Metriken pro Monat	3,00\$ pro Dashboard und Monat

Service	Kostenloses Kontingent	Preisgestaltung [USD]
Amazon CloudWatch — Alarme	10 Alarmmetriken (gilt nicht für hochauflösende Alarme)	<p>Die Standardauflösung (60 Sekunden) kostet 0,10\$ pro Alarmmetrik</p> <p>Hohe Auflösung (10 Sekunden) kostet 0,30 USD pro Alarmmetrik</p> <p>Die Erkennung von Anomalien mit Standardauflösung kostet 0,30 USD pro Alarm</p> <p>Die Erkennung von Anomalien mit hoher Auflösung kostet 0,90 USD pro Alarm</p> <p>Composite kostet 0,50\$ pro Alarm</p>
Amazon CloudWatch — Erfassung von Protokollen	5 GB Daten (Aufnahme, Archivierung und Daten, die durch Logs Insights-Abfragen gescannt wurden)	0,50\$ pro GB
Amazon CloudWatch — Speicherung von Protokollen	5 GB Daten (Aufnahme, Archivierung und Daten, die durch Logs Insights-Abfragen gescannt wurden)	0,005 USD pro GB gescannte r Daten
Amazon CloudWatch - Veranstaltungen	Alle Ereignisse außer benutzerdefinierten Ereignissen sind enthalten	1,00 USD pro Million Ereignisse für benutzerdefinierte Ereignisse 1,00 USD pro Million Ereignisse für kontoübergreifende Ereignisse
AWS Lambda - Anfragen	1 Million kostenlose Anfragen pro Monat	0,20\$ pro 1 Million Anfragen

Service	Kostenloses Kontingent	Preisgestaltung [USD]
AWS Lambda - Dauer	400.000 GB-Sekunden Rechenzeit pro Monat	0,0000166667\$ für jede GB-Sekunde. Der Preis für Duration hängt von der Speichermenge ab, die Sie Ihrer Funktion zuweisen. Sie können Ihrer Funktion eine beliebige Speichermenge zwischen 128 MB und 10.240 MB in Schritten von 1 MB zuweisen.
AWS Step Functions - Zustandsübergänge	4.000 kostenlose Zustandsübergänge pro Monat	Danach 0,025\$ pro 1.000 Zustandsübergänge
Amazon EventBridge	Alle von den AWS Diensten veröffentlichten Ereignisse zu Statusänderungen sind kostenlos	Benutzerdefinierte Ereignisse kosten 1,00 USD pro Million veröffentlichter benutzerdefinierter Ereignisse Veranstaltungen von Drittanbietern (SaaS) kosten 1,00 USD pro Million veröffentlichter Ereignisse Kontoübergreifende Ereignisse kosten 1,00 USD pro Million versendeter kontoübergreifender Ereignisse
Amazon SNS	Die ersten 1 Million SNS Amazon-Anfragen pro Monat sind kostenlos	Danach 0,50\$ pro 1 Million Anfragen
Amazon SQS	Die ersten 1 Million SQS Amazon-Anfragen pro Monat sind kostenlos	Danach 0,40\$ pro 1 Million bis 100 Milliarden Anfragen

Service	Kostenloses Kontingent	Preisgestaltung [USD]
Amazon-DynamoDB	Die ersten 25 GB Speicherplatz sind kostenlos	Danach 2,00\$ pro 1 Million konsistenter Lese- und Schreibvorgänge

Preisbeispiele (monatlich)

Beispiel 1: 300 Problembhebungen pro Monat

- 10 Konten, 1 Region
- 30 Abhilfemaßnahmen pro account/Region/month
- Gesamtkosten 21,17\$ pro Monat

Service	Annahmen	Monatliche Gebühren [USD]
AWS Systems Manager Automatisierung	Schritte: ~4 Schritte * 300 Korrekturmaßnahmen * 0,002\$ = 2,40\$ Dauer: 10 s * 300 Behebungen * 0,00003\$ = 0,09\$	2,49\$
AWS Security Hub	Es wurden keine kostenpflichtigen Dienste genutzt	\$0
CloudWatch Amazon-Protokolle	300 Abhilfemaßnahmen * 0,000002\$ = 0,0006\$ 0,0006\$ * 0,03 = 0,00018\$	< 0,01\$
AWS Lambda - Anfragen	300 Abhilfemaßnahmen * 6 Anfragen = 1.800 Anfragen 0,20\$ * 1.000.000 Anfragen = 0,20\$	0,20\$

Service	Annahmen	Monatliche Gebühren [USD]
AWS Lambda - Dauer	256 MB: 1,875 GB pro Sekunde * 300 Korrekturen * 0,0000167\$ = 0,009375\$	< 0,01\$
AWS Step Functions	17 Zustandsübergänge * 300 Korrekturen = 5.100 0,025\$ * (5.100/1.000) Zustandsübergänge = 0,15\$	0,15\$
EventBridge Amazon-Regeln	Keine Gebühr für Regeln	\$0
AWS Key Management Service	1 Schlüssel * 10 Konten * 1 Region * 1\$ = 10\$	10,00\$
Amazon-DynamoDB	2,00\$ * 1.000.000 Lese- und Schreibvorgänge = 2,00\$	2,00\$
Amazon SQS	0,40\$ * 1.000.000 Anfragen = 0,40\$	0,40\$
Amazon SNS	0,50\$ * 1.000.000 Benachrichtigungen = 0,50\$	0,50\$
Amazon CloudWatch — Metriken	0,30\$ * 7 benutzerdefinierte Metriken = 2,10\$ 0,01\$ * (300 * 3/1.000) Aufrufe von Put-Metriken = 0,01\$ API	2,11\$
Amazon CloudWatch — Dashboards	3,00\$ * 1 Dashboard = 3,00\$	3,00\$
Amazon CloudWatch — Alarme	0,10\$ * 3 Alarme = 0,30\$	0,30\$
Gesamt		21,17\$

Beispiel 2:3.000 Problembhebungen pro Monat

- 100 Konten, 1 Region
- 30 Abhilfemaßnahmen pro account/Region/month
- Gesamtkosten 134,86\$ pro Monat

Service	Annahmen	Monatliche Gebühren [USD]
AWS Systems Manager Automatisierung	Schritte: ~4 Schritte * 3.000 Korrekturmaßnahmen * 0,002\$ = 24,00\$ Dauer: 10 s * 3.000 Behebungen * 0,00003\$ = 0,90\$	24,90\$
AWS Security Hub	Es wurden keine kostenpfl ichtigen Dienste genutzt	\$0
CloudWatch Amazon-Pr otokolle	3.000 Korrekturmaßnahmen * 0,000002\$ = 0,006\$ 0,006\$ * 0,03 = 0,00018\$	< 0,01\$
AWS Lambda - Anfragen	3.000 Behebungen * 6 Anfragen = 18.000 Anfragen 0,20\$ * 1.000.000 Anfragen = 0,20\$	0,20\$
AWS Lambda - Dauer	256 MB: 1,875 GB pro Sekunde * 3.000 Korrekturen * 0,000167\$ = 0,09375\$	0,09\$
AWS Step Functions	17 Zustandsübergänge * 3.000 Korrekturen = 51.000	1,28\$

Service	Annahmen	Monatliche Gebühren [USD]
	0,025\$ * (51.000/1.000) Zustandsübergänge = 1,275\$	
EventBridge Amazon-Regeln	Keine Gebühr für Regeln	\$0
AWS Key Management Service	1 Schlüssel * 100 Konten * 1 Region * 1\$ = 100\$	100 USD
Amazon-DynamoDB	2,00\$ * 1.000.000 Lese- und Schreibvorgänge = 2,00\$	2,00\$
Amazon SQS	0,40\$ * 1.000.000 Anfragen = 0,40\$	0,40\$
Amazon SNS	0,50\$ * 1.000.000 Benachrichtigungen = 0,50\$	0,50\$
Amazon CloudWatch — Metriken	0,30\$ * 7 benutzerdefinierte Metriken = 2,10\$ 0,01\$ * (3000 * 3/1.000) Aufrufe von Put-Metriken = 0,09\$ API	2,19\$
Amazon CloudWatch — Dashboards	3,00\$ * 1 Dashboard = 3,00\$	3,00\$
Amazon CloudWatch — Alarme	0,10\$ * 3 Alarme = 0,30\$	0,30\$
Gesamt		134,86\$

Beispiel 3:30.000 Problembhebungen pro Monat

- 1.000 Konten, 1 Region
- 30 Abhilfemaßnahmen pro account/Region/month
- Gesamtkosten 1.281,01 USD pro Monat

Service	Annahmen	Monatliche Gebühren [USD]
AWS Systems Manager Automatisierung	Schritte: ~4 Schritte * 30.000 Korrekturmaßnahmen * 0,002\$ = 240,00\$ Dauer: 10 s * 30.000 Behebungen * 0,00003\$ = 9,00\$	249,00\$
AWS Security Hub	Es wurden keine kostenpflichtigen Dienste genutzt	\$0
CloudWatch Amazon-Protokolle	30.000 Behebungen * 0,000002\$ = 0,06\$ 0,06\$ * 0,03 = 0,0018\$	< 0,01\$
AWS Lambda - Anfragen	30.000 Behebungen * 6 Anfragen = 180.000 Anfragen 0,20\$ * 1.000.000 Anfragen = 0,20\$	0,20\$
AWS Lambda - Dauer	256 MB: 1,875 GB pro Sekunde * 30.000 Korrekturen * 0,000167\$ = 0,9375\$	0,94\$
AWS Step Functions	17 Zustandsübergänge * 30.000 Korrekturen = 510.000 0,025\$ * (510.000/1.000) Zustandsübergänge = 12,75\$	12,75\$
EventBridge Amazon-Regeln	Keine Gebühr für Regeln	\$0
AWS Key Management Service	1 Schlüssel * 1.000 Konten * 1 Region * 1 USD = 1.000 USD	1.000\$

Service	Annahmen	Monatliche Gebühren [USD]
Amazon-DynamoDB	0,000002\$ * 1.000.000 Lese- und Schreibvorgänge = 2,00\$	2,00\$
Amazon SQS	0,000004\$ * 1.000.000 Anfragen = 0,40\$	0,40\$
Amazon SNS	0,000005\$ * 1.000.000 Benachrichtigungen = 0,50\$	0,50\$
Amazon CloudWatch — Metriken	0,30\$ * 6 benutzerdefinierte Metriken = 1,80\$ 0,01\$ * (30.000 * 3/1.000) Aufrufe von Put-Metriken API = 0,90\$	2,70\$
Amazon CloudWatch — Dashboards	3,00\$ * 1 Dashboard = 3,00\$	3,00\$
Amazon CloudWatch — Alarme	0,10\$ * 2 Alarme = 0,20\$	0,20\$
Amazon CloudWatch — Einblicke in Anwendungen	0,10\$ x 40 Alarme (max.) = 4,00\$ 0,53\$ * 10 GB Protokolldaten (ca.) = 5,30\$ 0,00267\$ * 5 (geschätzt) OpsItems = ~0,01 \$	9,31\$
Gesamt		1.281,01\$

Zusätzliche Kosten für optionale Funktionen

In diesem Abschnitt werden die zusätzlichen Kosten aufgeführt, die mit optionalen Funktionen für diese Lösung verbunden sind.

Verbesserte CloudWatch Metriken

Wenn Sie den `EnableEnhancedCloudWatchMetricsParameter` `yes` bei der Bereitstellung des Admin-Stacks auswählen, erstellt die Lösung zwei benutzerdefinierte Metriken und einen Alarm für jede Kontroll-ID. Die Kosten hängen von der Anzahl der Kontrollen abIDs, die Sie korrigieren. In der folgenden Tabelle gehen wir davon aus, dass Sie alle 96 verschiedenen Kontrollen IDs pro Monat korrigieren, um die Obergrenze der Kosten zu ermitteln.

Service	Annahmen	Monatliche Gebühren [USD]
	96 Kontrolle IDs * 2 = 192 benutzerdefinierte Metriken	
Amazon CloudWatch — Metriken	0,30\$ * 192 benutzerdefinierte Metriken = 57,60\$	57,60\$
Amazon CloudWatch — Alarme	0,10\$ * 96 Alarme = 9,60\$	9,60\$
Gesamt		67,20\$

CloudTrail Aktionsprotokoll

In jedem Mitgliedskonto, für das Sie die Aktionsprotokollfunktion aktivieren, erstellt die Lösung einen CloudTrail Pfad, in dem alle Schreibverwaltungsereignisse protokolliert werden. Eine Lambda-Funktion filtert Ereignisse heraus, die nichts mit der Lösung zu tun haben. Das bedeutet, dass sich die Kosten auf die Gesamtzahl der Verwaltungsereignisse in Ihrem Konto beziehen, da Ereignisse, die nichts mit der Lösung zu tun haben, weiterhin im Trail erfasst und von der Lambda-Funktion verarbeitet werden.

Für die folgende Tabelle gehen wir von 150.000 Verwaltungsereignissen pro Monat in Ihrem Konto aus. Die tatsächlichen Kosten hängen von der tatsächlichen Aktivität der Verwaltungsereignisse in Ihrem Konto ab.

Service	Annahmen	Monatliche Gebühren [USD]
AWS CloudTrail	150.000\$ * 2,00/100.000 \$ = 3,00\$	3,00\$

Service	Annahmen	Monatliche Gebühren [USD]
Lambda	$150.000 * 0,2 * 0,125 = 3.750$ GB-Sekunden $3.750 * 0,0000166667\$ =$ $0,0625\$$ Rechenzeit $0,15 * 0,20\$ = 0,03\$$ Anforderu ngskosten $0,0625\$ + 0,03\$ = 0,0952\$$ Gesamtkosten für Lambda	0,0925\$
Gesamt		3,09\$ pro Mitgliedskonto

Sicherheit

Wenn Sie Systeme auf der AWS Infrastruktur aufbauen, teilen Sie sich die Sicherheitsverantwortung zwischen Ihnen und AWS. Dieses [gemeinsame Modell](#) reduziert Ihren betrieblichen Aufwand, da AWS die Komponenten wie das Host-Betriebssystem, die Virtualisierungsebene und die physische Sicherheit der Einrichtungen, in denen die Services ausgeführt werden, betrieben, verwaltet und kontrolliert werden. Weitere Informationen zur AWS Sicherheit finden Sie unter [AWS Cloud Security](#).

IAM-Rollen

AWS Identity and Access Management Zugriffsmanagement-Rollen (IAM) ermöglichen es Kunden, Diensten und Benutzern in der AWS Cloud detaillierte Zugriffsrichtlinien und -berechtigungen zuzuweisen. Diese Lösung erstellt IAM Rollen, die den automatisierten Funktionen der Lösung Zugriff gewähren, sodass sie innerhalb eines engen, für jede Problembehebung spezifischen Berechtigungsumfangs Korrekturmaßnahmen durchführen können.

Die Step-Funktion des Administratorkontos ist der Rolle SO0111- zugewiesen. SHARR-Orchestrator-Admin Nur diese Rolle darf das SO0111-Orchestrator-Mitglied in jedem Mitgliedskonto übernehmen. Die Mitgliedsrolle darf von jeder Wartungsrolle an den AWS Systems Manager Manager-Dienst übergeben werden, um bestimmte Wartungs-Runbooks auszuführen. Die Namen der Wartungsrollen beginnen mit SO0111, gefolgt von einer Beschreibung, die dem Namen des Wartungs-Runbooks

entspricht. SO0111-R `emoveVPCDefault SecurityGroupRules` ist beispielsweise die Rolle für das -R Remediation Runbook. ASR `emoveVPCDefault SecurityGroupRules`

Unterstützt AWS-Regionen

Name der Region	Regionscode
USA Ost (Ohio)	us-east-2
USA Ost (Nord-Virginia)	us-east-1
USA West (Nordkalifornien)	us-west-1
USA West (Oregon)	us-west-2
Afrika (Kapstadt)	af-south-1
Asien-Pazifik (Hongkong)	ap-east-1
Asien-Pazifik (Hyderabad)	ap-south-2
Asien-Pazifik (Jakarta)	ap-southeast-3
Asien-Pazifik (Melbourne)	ap-southeast-4
Asien-Pazifik (Mumbai)	ap-south-1
Asien-Pazifik (Osaka)	ap-northeast-3
Asien-Pazifik (Seoul)	ap-northeast-2
Asien-Pazifik (Singapur)	ap-southeast-1
Asien-Pazifik (Sydney)	ap-southeast-2
Asien-Pazifik (Tokio)	ap-northeast-1
Kanada (Zentral)	ca-central-1
Europa (Frankfurt)	eu-central-1

Name der Region	Regionscode
Europa (Irland)	eu-west-1
Europa (London)	eu-west-2
Europa (Mailand)	eu-south-1
Europa (Paris)	eu-west-3
Europa (Spanien)	eu-south-2
Europa (Stockholm)	eu-north-1
Europa (Zürich)	eu-central-2
Naher Osten (Bahrain)	me-south-1
Naher Osten () UAE	me-central-1
Südamerika (São Paulo)	sa-east-1
AWS GovCloud (US-Ost)	us-gov-east-1
AWS GovCloud (US-West)	us-gov-east-2
China (Beijing)	cn-north-1
China (Ningxia)	cn-northwest-1

Kontingente

Servicekontingente, auch als Limits bezeichnet, sind die maximale Anzahl von Serviceressourcen oder -vorgängen für Ihr AWS-Konto.

Kontingente für AWS Dienste in dieser Lösung

Stellen Sie sicher, dass Sie über ein ausreichendes Kontingent für jeden der [in dieser Lösung implementierten Dienste](#) verfügen. Weitere Informationen finden Sie unter [AWSDienstkontingente](#).

Verwenden Sie die folgenden Links, um zur Seite für diesen Dienst zu gelangen. Um die Service Quotas für alle AWS Dienste in der Dokumentation anzuzeigen, ohne zwischen den Seiten zu wechseln, sehen Sie sich PDF stattdessen die Informationen auf der Seite [Dienstendpunkte und Kontingente](#) in der an.

AWS CloudFormation Kontingente

Ihr AWS Konto verfügt über AWS CloudFormation Kontingente, die Sie beachten sollten, wenn Sie [den Stack in dieser Lösung starten](#). Wenn Sie diese Kontingente verstehen, können Sie Limitationsfehler vermeiden, die Sie daran hindern würden, diese Lösung erfolgreich einzusetzen. Weitere Informationen finden Sie unter [AWS CloudFormation Kontingente](#) im AWS CloudFormation - Benutzerhandbuch.

Amazon EventBridge regelt Kontingente

Ihr AWS Konto verfügt über Kontingente nach EventBridge Amazon-Regeln, die Sie beachten sollten, wenn Sie die Playbooks auswählen, die mit der Lösung bereitgestellt werden sollen. Jedes Playbook erstellt eine EventBridge Regel für jede Kontrolle, die es korrigieren kann. Beim Einsatz mehrerer Playbooks ist es möglich, das Regelkontingent zu erreichen. Weitere Informationen finden Sie unter [EventBridge Amazon-Kontingente](#) im EventBridge Amazon-Benutzerhandbuch.

AWSBereitstellung von Security Hub

AWSDie Bereitstellung und Konfiguration von Security Hub ist eine Voraussetzung für diese Lösung. Weitere Informationen zur Einrichtung von AWS Security Hub finden Sie unter [AWSSecurity Hub einrichten](#) im AWSSecurity Hub Hub-Benutzerhandbuch.

In Ihrem Hauptkonto muss mindestens ein funktionierender Security Hub konfiguriert sein. Sie können diese Lösung in demselben Konto (und derselben AWS Region) wie das Security Hub-Primärkonto bereitstellen. In jedem primären und sekundären Security Hub Hub-Konto müssen Sie außerdem die Mitgliedsvorlage bereitstellen, die AssumeRole Berechtigungen für die AWS Step Functions der Lösung zur Ausführung von Behebungsrunbooks im Konto gewährt.

Stack im Vergleich zur Bereitstellung StackSets

Mit einem Stack-Set können Sie mithilfe einer einzigen Vorlage Stapel in AWS Konten in verschiedenen AWS Regionen erstellen. AWS CloudFormation Ab Version 1.4 unterstützt diese Lösung die Bereitstellung von Stacksets, indem Ressourcen je nachdem, wo und wie sie

bereitgestellt werden, aufgeteilt werden. Kunden mit mehreren Konten, insbesondere solche, die diese verwenden AWS Organizations, können von der Verwendung von Stack-Sets für die Bereitstellung auf vielen Konten profitieren. Dadurch wird der Aufwand für die Installation und Wartung der Lösung reduziert. Weitere Informationen zu StackSets finden Sie unter [Verwenden von AWS CloudFormation StackSets](#).

Stellen Sie die Lösung bereit

Important

Wenn die Funktion für [konsolidierte Kontrollergebnisse](#) in Security Hub aktiviert ist (dies ist die Standardeinstellung in neuen Bereitstellungen), aktivieren Sie bei der Bereitstellung dieser Lösung nur das Security Control (CS) -Playbook. Wenn die Funktion nicht aktiviert ist, aktivieren Sie nur die Playbooks für die Sicherheitsstandards, die in Security Hub aktiviert sind. Die Aktivierung zusätzlicher Playbooks kann dazu führen, dass das [Kontingent für EventBridge](#) Regeln erreicht wird.

Diese Lösung verwendet [AWS CloudFormation Vorlagen und Stacks](#), um ihre Bereitstellung zu automatisieren. Die CloudFormation Vorlagen spezifizieren die in dieser Lösung enthaltenen AWS Ressourcen und ihre Eigenschaften. Der CloudFormation Stack stellt die Ressourcen bereit, die in den Vorlagen beschrieben sind.

Damit die Lösung funktioniert, müssen drei Vorlagen bereitgestellt werden. Entscheiden Sie zunächst, wo die Vorlagen bereitgestellt werden sollen, und entscheiden Sie dann, wie sie bereitgestellt werden sollen.

In dieser Übersicht werden die Vorlagen beschrieben und es wird beschrieben, wie entschieden wird, wo und wie sie eingesetzt werden sollen. In den nächsten Abschnitten finden Sie detailliertere Anweisungen zum Bereitstellen der einzelnen Stacks als Stack oder StackSet.

Entscheiden, wo jeder Stack eingesetzt werden soll

Die drei Vorlagen werden mit den folgenden Namen bezeichnet und enthalten die folgenden Ressourcen:

- Admin-Stack: Orchestrator-Schrittfunktion, Ereignisregeln und benutzerdefinierte Security Hub Hub-Aktion.
- Mitgliederliste: Dokumente zur SSM Automatisierung von Problembehebungen.
- Rollenstapel für Mitglieder: IAM Rollen für Problembehebungen.

Der Admin-Stack muss einmal in einem einzigen Konto und in einer einzigen Region bereitgestellt werden. Es muss in dem Konto und der Region bereitgestellt werden, die Sie als Aggregationsziel für Security Hub Hub-Ergebnisse für Ihre Organisation konfiguriert haben.

Die Lösung arbeitet mit Security Hub-Ergebnissen, sodass sie nicht mit Ergebnissen aus einem bestimmten Konto und einer bestimmten Region arbeiten kann, wenn dieses Konto oder diese Region nicht so konfiguriert wurde, dass Ergebnisse im Security Hub-Administratorkonto und in der Region zusammengefasst werden.

Beispielsweise hat eine Organisation Konten, die in Regionen betrieben werden `us-west-2`, `us-east-1` und hat mit einem Konto `111111111111` als Security Hub einen delegierten Administrator in `Regionus-east-1`. Konten `222222222222` und `333333333333` müssen Security Hub Hub-Mitgliedskonten für das delegierte Administratorkonto `111111111111` sein. Alle drei Konten müssen so konfiguriert sein, dass sie die Ergebnisse von `us-west-2` bis `us-east-1` aggregieren. Der Admin-Stack muss für das Konto `111111111111` in `Regionus-east-1` bereitgestellt werden.

Weitere Informationen zur Suche nach Aggregation finden Sie in der Dokumentation zu [delegierten Security Hub-Administratorkonten](#) und [regionsübergreifender](#) Aggregation.

Der Admin-Stack muss zuerst die Bereitstellung abschließen, bevor die Mitglieds-Stacks bereitgestellt werden, damit eine Vertrauensbeziehung zwischen den Mitgliedskonten und dem Hub-Konto hergestellt werden kann.

Der Mitglieds-Stack muss für jedes Konto und jede Region bereitgestellt werden, in der Sie Fehler korrigieren möchten. Dazu kann das delegierte Security Hub-Administratorkonto gehören, in dem Sie zuvor den ASR Admin-Stack bereitgestellt haben. Die Automatisierungsdokumente müssen in den Mitgliedskonten ausgeführt werden, um das kostenlose Kontingent für Automation nutzen zu können.
SSM

Wenn Sie anhand des vorherigen Beispiels Ergebnisse aus allen Konten und Regionen korrigieren möchten, muss der Mitgliederstapel für alle drei Konten (`111111111111222222222222`, `und333333333333`) und beide Regionen (`us-east-1` `us-west-2`) bereitgestellt werden.

Der Mitgliederrollen-Stack muss für jedes Konto bereitgestellt werden, er enthält jedoch globale Ressourcen (IAM Rollen), die nur einmal pro Konto bereitgestellt werden können. Es spielt keine Rolle, in welcher Region Sie den Mitgliederrollen-Stack bereitstellen. Der Einfachheit halber empfehlen wir daher, ihn in derselben Region bereitzustellen, in der der Admin-Stack bereitgestellt wird.

Unter Verwendung des vorherigen Beispiels empfehlen wir, den Mitgliederrollen-Stack für alle drei Konten (111111111111222222222222, und333333333333) in bereitzustellenus-east-1.

Entscheiden Sie, wie die einzelnen Stacks bereitgestellt werden

Die Optionen für die Bereitstellung eines Stacks sind

- CloudFormation StackSet (selbstverwaltete Berechtigungen)
- CloudFormation StackSet (vom Service verwaltete Berechtigungen)
- CloudFormation Stapel

StackSets mit vom Service verwalteten Berechtigungen sind am praktischsten, da sie nicht die Bereitstellung eigener Rollen erfordern und automatisch für neue Konten in der Organisation bereitgestellt werden können. Leider unterstützt diese Methode keine verschachtelten Stacks, die wir sowohl im Admin-Stack als auch im Member-Stack verwenden. Der einzige Stack, der auf diese Weise bereitgestellt werden kann, ist der Stack der Mitgliedsrollen.

Beachten Sie, dass bei der Bereitstellung für die gesamte Organisation das Organisationsverwaltungs-konto nicht enthalten ist. Wenn Sie also Fehler im Organisationsverwaltungs-konto korrigieren möchten, müssen Sie die Bereitstellung für dieses Konto separat durchführen.

Der Mitgliederstapel muss für jedes Konto und jede Region bereitgestellt werden, kann jedoch nicht StackSets mit vom Dienst verwalteten Berechtigungen bereitgestellt werden, da er verschachtelte Stacks enthält. Wir empfehlen daher, diesen Stack StackSets mit selbstverwalteten Berechtigungen bereitzustellen.

Der Admin-Stack wird nur einmal bereitgestellt, sodass er als einfacher CloudFormation Stack oder StackSet mit selbstverwalteten Berechtigungen in einem einzigen Konto und einer Region bereitgestellt werden kann.

Konsolidierte Kontrollergebnisse

Die Konten in Ihrer Organisation können so konfiguriert werden, dass die Funktion für konsolidierte Kontrollergebnisse von Security Hub aktiviert oder deaktiviert wird. Weitere Informationen finden Sie im AWS Security Hub Benutzerhandbuch unter [Konsolidierte Kontrollergebnisse](#).

⚠ Important

Wenn diese Option aktiviert ist, müssen Sie Version 2.0.0 der Lösung oder höher verwenden. Darüber hinaus müssen Sie sowohl die verschachtelten Stacks Admin als auch Member für die Standards „SC“ oder „Security Control“ bereitstellen. Dadurch werden die Automatisierungsdokumente und EventBridge -regeln für die Verwendung mit der konsolidierten Steuerung bereitgestellt, die beim IDs Aktivieren dieser Funktion generiert wird. Bei Verwendung dieser Funktion müssen die verschachtelten Stacks Admin oder Member nicht für bestimmte Standards bereitgestellt werden (z. B. AWSFSBP).

AWS CloudFormation Vorlagen

[View template](#)

aws-

[sharr-deploy](#).template — Verwenden Sie diese Vorlage, um die automatische Sicherheitsreaktion auf die Lösung zu starten. AWS Die Vorlage installiert die Kernkomponenten der Lösung, einen verschachtelten Stack für die AWS Step Functions Protokolle und einen verschachtelten Stack für jeden Sicherheitsstandard, den Sie aktivieren möchten.

Zu den verwendeten Diensten gehören Amazon Simple Notification Service AWS Key Management Service AWS Identity and Access Management, AWS Lambda, AWS Step Functions,, Amazon CloudWatch Logs, Amazon S3 und AWS Systems Manager.

Unterstützung für Administratorkonten

Die folgenden Vorlagen sind im AWS Security Hub-Administratorkonto installiert, um die Sicherheitsstandards zu aktivieren, die Sie unterstützen möchten. Sie können wählen, welche der folgenden Vorlagen Sie bei der Installation von installieren möchten `aws-sharr-deploy.template`.

`aws-sharr-orchestrator-log.template` — Erstellt eine CloudWatch Protokollgruppe für die Orchestrator-Step-Funktion.

`AFSBPStack.template` — Regeln der Version 1.0.0 mit den AWS grundlegenden bewährten Sicherheitsmethoden.

`CIS120stack.Template` — Benchmarks der CIS Amazon Web Services Foundation, Regeln für Version 1.2.0.

CIS140stack.Template — Benchmarks der CIS Amazon Web Services Foundations, v1.4.0-Regeln.

PCI321Stack.template - - v3.2.1-Regeln. PCI DSS

NISTStack.template - Nationales Institut für Standards und Technologie (NIST), Regeln für Version 5.0.0.

SCStack.template — Regeln für SC v2.0.0.

Mitgliedskonten

[View template](#)

aws-

[sharr-member](#).template — Verwenden Sie diese Vorlage, nachdem Sie die Kernlösung eingerichtet haben, um AWS Systems Manager Manager-Automatisierungsrunbooks und -Berechtigungen in jedem Ihrer AWS Security Hub Hub-Mitgliedskonten (einschließlich des Administratorkontos) zu installieren. Mit dieser Vorlage können Sie auswählen, welche Playbooks nach Sicherheitsstandards installiert werden sollen.

Die `aws-sharr-member.template` installiert die folgenden Vorlagen auf der Grundlage Ihrer Auswahl:

`aws-sharr-remediations.template` — Allgemeiner Problembehebungscode, der von einem oder mehreren Sicherheitsstandards verwendet wird.

`AFSBPMemberStack.template` — Runbooks für Einstellungen, Berechtigungen und Problembehebungen in der Version 1.0.0 für AWS grundlegende Sicherheitsverfahren.

`CIS120 MemberStack .template` — Benchmarks der CIS Amazon Web Services Foundations, Einstellungen, Berechtigungen und Reparatur-Runbooks für Version 1.2.0.

`CIS140 MemberStack .template` — Benchmarks der CIS Amazon Web Services Foundations, Einstellungen, Berechtigungen und Problembehebungs-Runbooks für Version 1.4.0.

`PCI321MemberStack.template` - PCI - Runbooks für Einstellungen, Berechtigungen und Problembehebungen der DSS Version v3.2.1.

`NISTMemberStack.template` — Runbooks für Einstellungen, Berechtigungen und Problembehebung des National Institute of Standards and Technology (NIST), Version 5.0.0.

`SCMemberStack.template` — Runbooks für Einstellungen, Berechtigungen und Problembehebungen für die Sicherheitskontrolle.

Rollen der Mitglieder

[View template](#)

aws-

[sharr-member-roles](#).template — Definiert die Korrekturrollen, die in jedem AWS Security Hub Mitgliedskonto benötigt werden.

Integration des Ticketsystems

Verwenden Sie eine der folgenden Vorlagen, um sie in Ihr Ticketsystem zu integrieren.

[View template](#)

JiraBlu

— Bereitstellen, wenn Sie Jira als Ticketsystem verwenden.

[View template](#)

Service

— Bereitstellen, wenn Sie es ServiceNow als Ticketsystem verwenden.

Wenn Sie ein anderes externes Ticketsystem integrieren möchten, können Sie einen dieser Stacks als Vorlage verwenden, um zu verstehen, wie Sie Ihre eigene benutzerdefinierte Integration implementieren können.

Automatisierte Bereitstellung - StackSets

Note

Wir empfehlen die Bereitstellung mit StackSets. Für Bereitstellungen mit einem einzigen Konto oder zu Test- oder Evaluierungszwecken sollten Sie jedoch die [Bereitlungsoption Stacks](#) in Betracht ziehen.

Bevor Sie die Lösung auf den Markt bringen, sollten Sie sich mit der Architektur, den Lösungskomponenten, der Sicherheit und den Entwurfsüberlegungen vertraut machen, die in diesem Handbuch behandelt werden. Folgen Sie den step-by-step Anweisungen in diesem Abschnitt, um die Lösung zu konfigurieren und in Ihrem System bereitzustellen AWS Organizations.

Bereitstellungszeit: Ungefähr 30 Minuten pro Konto, abhängig von den StackSet Parametern.

Voraussetzungen

[AWS Organizations](#) hilft Ihnen dabei, Ihre AWS Umgebung und Ressourcen mit mehreren Konten zentral zu verwalten und zu steuern. StackSets funktioniert am besten mit AWS Organizations.

Wenn Sie bereits Version 1.3.x oder eine frühere Version dieser Lösung bereitgestellt haben, müssen Sie die bestehende Lösung deinstallieren. Weitere Informationen finden Sie unter Lösung [aktualisieren](#).

Bevor Sie diese Lösung bereitstellen, überprüfen Sie Ihre AWS Security Hub Hub-Bereitstellung:

- In Ihrer AWS Organisation muss es ein delegiertes Security Hub-Administratorkonto geben.
- Security Hub sollte so konfiguriert sein, dass die Ergebnisse regionsübergreifend zusammengefasst werden. Weitere Informationen finden Sie unter [Aggregieren von Ergebnissen in verschiedenen Regionen](#) im AWS Security Hub Hub-Benutzerhandbuch.
- Sie sollten [Security Hub für Ihr Unternehmen in jeder Region aktivieren](#), in der Sie es AWS nutzen.

Bei diesem Verfahren wird davon ausgegangen, dass Sie mehrere Konten bei AWS Organizations haben und ein AWS Organizations Administratorkonto und ein AWS Security Hub-Administratorkonto delegiert haben.

Überblick über die Bereitstellung

Note

StackSets Bei der Bereitstellung dieser Lösung wird eine Kombination aus serviceverwaltetem und StackSets selbstverwaltetem System verwendet. Self-Managed StackSets muss derzeit verwendet werden, da sie Nested verwenden StackSets, die bei Service-Managed noch nicht unterstützt werden. StackSets

Stellen Sie das StackSets von einem [delegierten Administratorkonto](#) in Ihrem bereit. AWS Organizations

Planung

Verwenden Sie das folgende Formular, um bei der StackSets Bereitstellung zu helfen. Bereiten Sie Ihre Daten vor und kopieren Sie dann die Werte und fügen Sie sie während der Bereitstellung ein.

```
AWS Organizations admin account ID: _____
Security Hub admin account ID: _____
CloudTrail Logs Group: _____
Member account IDs (comma-separated list):
_____,
_____,
_____,
_____,
_____,
AWS Organizations OUs (comma-separated list):
_____,
_____,
_____,
_____,
_____
```

(Optional) Schritt 0: Stellen Sie den Ticketing-Integrationsstapel bereit

- Wenn Sie die Ticketing-Funktion verwenden möchten, stellen Sie zuerst den Ticketing-Integrations-Stack in Ihrem Security Hub-Administratorkonto bereit.
- Kopieren Sie den Namen der Lambda-Funktion aus diesem Stack und stellen Sie ihn als Eingabe für den Admin-Stack bereit (siehe Schritt 1).

Schritt 1: Starten Sie den Admin-Stack im delegierten Security Hub-Administratorkonto

- Starten Sie die `aws-sharr-deploy.template` AWS CloudFormation Vorlage mithilfe eines selbstverwalteten StackSet Systems in Ihrem AWS Security Hub-Administratorkonto in derselben Region wie Ihr Security Hub-Administrator. Diese Vorlage verwendet verschachtelte Stacks.
- Wählen Sie aus, welche Sicherheitsstandards installiert werden sollen. Standardmäßig ist nur SC ausgewählt (empfohlen).
- Wählen Sie eine vorhandene Orchestrator-Protokollgruppe aus, die Sie verwenden möchten. Wählen Sie `Yes`, ob diese `S00111-SHARR-Orchestrator` bereits in einer früheren Installation vorhanden ist.

Weitere Informationen zur Selbstverwaltung StackSets finden Sie unter [Gewähren von selbstverwalteten Berechtigungen](#) im AWS CloudFormation Benutzerhandbuch.

Schritt 2: Installieren Sie die Behebungsrollen in jedem Mitgliedskonto AWS Security Hub

Warten Sie, bis Schritt 1 die Bereitstellung abgeschlossen hat, da die Vorlage in Schritt 2 auf IAM Rollen verweist, die in Schritt 1 erstellt wurden.

- Starten Sie die `aws-sharr-member-roles.template` AWS CloudFormation Vorlage mithilfe eines vom Service verwalteten StackSet Systems in einer einzelnen Region in jedem Konto in Ihrer AWS Organizations.
- Wählen Sie, ob diese Vorlage automatisch installiert werden soll, wenn ein neues Konto der Organisation beitrifft.
- Geben Sie die Konto-ID Ihres AWS Security Hub Administratorkontos ein.

Schritt 3: Starten Sie den Mitglieds-Stack für jedes AWS Security Hub-Mitgliedskonto und jede Region

- Starten Sie die `aws-sharr-member.template` AWS CloudFormation Vorlage mithilfe von Selbstverwaltung in allen Regionen StackSets, in denen Sie AWS Ressourcen in jedem Konto Ihrer AWS Organisation haben, das von demselben Security Hub-Administrator verwaltet wird.

Note

Bis Service-Managed Nested Stacks StackSets unterstützt, müssen Sie diesen Schritt für alle neuen Konten ausführen, die der Organisation beitreten.

- Wählen Sie aus, welche Security Standard-Playbooks installiert werden sollen.
- Geben Sie den Namen einer CloudTrail Protokollgruppe an (die bei einigen Problembehebungen verwendet wird).
- Geben Sie die Konto-ID Ihres AWS Security Hub Administratorkontos ein.

(Optional) Schritt 0: Starten Sie einen Ticketsystem-Integrationsstapel

1. Wenn Sie die Ticketing-Funktion verwenden möchten, starten Sie zuerst den entsprechenden Integrationsstapel.
2. Wählen Sie die bereitgestellten Integrations-Stacks für Jira oder verwenden Sie sie als Vorlage ServiceNow, um Ihre eigene benutzerdefinierte Integration zu implementieren.

So stellen Sie den Jira-Stack bereit:

- a. Geben Sie einen Namen für Ihren Stack ein.

- b. Stellen Sie das URI Ihrer Jira-Instanz zur Verfügung.
- c. Geben Sie den Projektschlüssel für das Jira-Projekt ein, an das Sie Tickets senden möchten.
- d. Erstellen Sie in Secrets Manager ein neues Key-Value-Secret, das Ihre Username Jira und enthält. Password

**Note**

Sie können einen API Jira-Schlüssel anstelle Ihres Passworts verwenden, indem Sie Ihren Benutzernamen als Username und Ihren API Schlüssel als angeben. Password

- e. Fügen Sie ARN dieses Geheimnis als Eingabe zum Stack hinzu.

Specify stack details

Provide a stack name**Stack name**

Stack name must be 1 to 128 characters, start with a letter, and only contain alphanumeric characters. Character count: 22/128.

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

Jira Project Information**InstanceURI**

The URI of your Jira instance. For example: <https://my-jira-instance.atlassian.net>

JiraProjectKey

The key of your Jira project where tickets will be created.

Jira API Credentials**SecretArn**

The ARN of the Secrets Manager secret where you have stored your API credentials. This must be a JSON secret with the following keys: Username,Password.

[Cancel](#)[Previous](#)[Next](#)

Um den Stack bereitzustellen: ServiceNow

- a. Geben Sie einen Namen für Ihren Stack ein.
- b. Geben Sie den URI Ihrer ServiceNow Instanz an.

- c. Geben Sie Ihren ServiceNow Tabellennamen an.
- d. Erstellen Sie einen API Schlüssel ServiceNow mit der Berechtigung, die Tabelle zu ändern, in die Sie schreiben möchten.
- e. Erstellen Sie in Secrets Manager ein Geheimnis mit dem Schlüssel API_Key und geben Sie das Geheimnis ARN als Eingabe für den Stack an.

Specify stack details

Provide a stack name

Stack name

Stack name must be 1 to 128 characters, start with a letter, and only contain alphanumeric characters. Character count: 19/128.

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

ServiceNow Project Information

InstanceURI
The URI of your ServiceNow instance. For example: `https://my-servicenow-instance.service-now.com`

ServiceNowTableName
Enter the name of your ServiceNow Table where tickets should be created.

ServiceNow API Credentials

SecretArn
The ARN of the Secrets Manager secret where you have stored your API credentials. This must be a JSON secret with the following keys: `API_Key`.

[Cancel](#) [Previous](#) [Next](#)

So erstellen Sie einen benutzerdefinierten Integrationsstapel: Fügen Sie eine Lambda-Funktion hinzu, die der Solution Orchestrator Step Functions für jede Korrektur aufrufen kann. Die Lambda-Funktion sollte die von Step Functions bereitgestellten Eingaben verwenden, eine Payload gemäß den Anforderungen Ihres Ticketsystems erstellen und eine Anfrage an Ihr System stellen, um das Ticket zu erstellen.

Schritt 1: Starten Sie den Admin-Stack im delegierten Security Hub-Administratorkonto

1. Starten Sie den [Admin-Stack](#) mit Ihrem Security Hub-Administratorkonto. `aws-sharr-deploy.template` In der Regel eines pro Organisation in einer einzigen Region. Da dieser Stack verschachtelte Stacks verwendet, müssen Sie diese Vorlage als selbstverwaltete Vorlage bereitstellen. StackSet

Configure StackSet options

Tags

You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack.

Key	Value	Remove
-----	-------	--------

Permissions

Choose an IAM role to explicitly define how CloudFormation will manage your target accounts. If you don't choose a role, CloudFormation uses permissions based on your user credentials. [Learn more](#)

Service-managed permissions
StackSets automatically configures the permissions required to deploy to target accounts managed by AWS Organizations. With this option, you can enable automatic deployment to accounts in your organization

Self-service permissions
You create the execution roles required to deploy to target accounts

IAM admin role ARN - optional

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role name	AWSCloudFormationStackSetAdministrationRole	Remove
---------------	---	--------

⚠ StackSets will use this role for administering your individual accounts.

IAM execution role name

AWSCloudFormationStackSetExecutionRole
--

IAM execution role name can include letters (A-Z and a-z), numbers (0-9), and select special characters (+,=,@,-_) characters. Maximum length is 64 characters.

Cancel Previous **Next**

StackSet Optionen konfigurieren

2. Geben Sie für den Parameter Kontonummern die Konto-ID des AWS Security Hub-Administratorkontos ein.
3. Wählen Sie für den Parameter Regionen angeben nur die Region aus, in der der Security Hub-Administrator aktiviert ist. Warten Sie, bis dieser Schritt abgeschlossen ist, bevor Sie mit Schritt 2 fortfahren.

Schritt 2: Installieren Sie die Behebungsrollen in jedem AWS Security Hub-Mitgliedskonto

Verwenden Sie einen vom Service verwalteten Dienst StackSets , um die [Vorlage für Mitgliederrollen](#) bereitzustellen. `aws-sharr-member-roles.template` Diese StackSet muss in einer Region pro Mitgliedskonto bereitgestellt werden. Es definiert die globalen Rollen, die kontenübergreifende API Aufrufe von der SHARR Orchestrator-Step-Funktion aus ermöglichen.

1. Stellen Sie die Lösung gemäß den Richtlinien Ihrer Organisation in der gesamten Organisation (in der Regel) oder in verschiedenen Organisationseinheiten bereit.
2. Aktivieren Sie die automatische Bereitstellung, damit neue Konten in den AWS Organizations diese Berechtigungen erhalten.
3. Wählen Sie für den Parameter Regionen angeben eine einzelne Region aus. IAMRollen sind global. Während der StackSet Bereitstellung können Sie mit Schritt 3 fortfahren.

Specify StackSet details

StackSet name

StackSet name

Must contain only letters, numbers, and dashes. Must start with a letter.

StackSet description

You can use the description to identify the stack set's purpose or other important information.

StackSet description

Parameters (1)

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

SecHubAdminAccount
Admin account number

Cancel Previous **Next**

Geben Sie StackSet Einzelheiten an

Schritt 3: Starten Sie den Mitglieds-Stack für jedes AWS Security Hub-Mitgliedskonto und jede Region

Da der [Mitglieds-Stack](#) verschachtelte Stacks verwendet, müssen Sie ihn als selbstverwalteter Stack bereitstellen. StackSet Die automatische Bereitstellung für neue Konten in der Organisation wird dadurch nicht unterstützt. AWS

Parameter

LogGroup Konfiguration: Wählen Sie die Protokollgruppe aus, die CloudTrail Protokolle empfängt. Wenn keine vorhanden ist oder wenn die Protokollgruppe für jedes Konto unterschiedlich ist, wählen Sie einen geeigneten Wert. Kontoadministratoren müssen den Systems Manager LogGroupName Manager-Parameter Store /Solutions/SO0111/Metrics _ aktualisieren, nachdem sie eine CloudWatch Protokollgruppe für CloudTrail Protokolle erstellt haben. Dies ist für Problembhebungen erforderlich, bei denen bei API Anrufen Messwertalarne generiert werden.

Standards: Wählen Sie die Standards aus, die in das Mitgliedskonto geladen werden sollen. Dadurch werden nur die AWS Systems Manager Manager-Runbooks installiert — der Sicherheitsstandard wird nicht aktiviert.

SecHubAdminAccount: Geben Sie die Konto-ID des AWS Security Hub-Administratorkontos ein, auf dem Sie die Admin-Vorlage der Lösung installiert haben.

The screenshot shows the 'Accounts' configuration page in the AWS CloudFormation console. The page title is 'Accounts' with the subtitle 'Identify accounts or organizational units in which you want to modify stacks'. Under 'Deployment locations', there are two radio buttons: 'Deploy stacks in accounts' (which is selected) and 'Deploy stacks in organizational units'. Below this, the 'Account numbers' section has a text input field containing '111122223333, 123456789012, 111144442222'. A note below the field states '12-Digit account numbers separated by commas.' At the bottom, there is an 'Upload .csv file' button with a file icon and the text 'No file chosen'.

Konten

Bereitstellungsorte: Sie können eine Liste mit Kontonummern oder Organisationseinheiten angeben.

Regionen angeben: Wählen Sie alle Regionen aus, in denen Sie die Ergebnisse korrigieren möchten. Sie können die Bereitstellungsoptionen entsprechend der Anzahl der Konten und Regionen anpassen. Die Parallelität der Regionen kann parallel sein.

Automatisierte Bereitstellung — Stacks

Note

Für Kunden mit mehreren Konten empfehlen wir dringend die [Bereitstellung mit StackSets](#).

Bevor Sie die Lösung auf den Markt bringen, sollten Sie sich mit der Architektur, den Lösungskomponenten, der Sicherheit und den Entwurfsüberlegungen vertraut machen, die in diesem Handbuch behandelt werden. Folgen Sie den step-by-step Anweisungen in diesem Abschnitt, um die Lösung zu konfigurieren und in Ihrem Konto bereitzustellen.

Zeit für die Bereitstellung: Ungefähr 30 Minuten

Voraussetzungen

Bevor Sie diese Lösung bereitstellen, stellen Sie sicher, dass sie AWS Security Hub sich in derselben AWS Region wie Ihr primäres und sekundäres Konto befindet. Wenn Sie diese Lösung bereits bereitgestellt haben, müssen Sie die bestehende Lösung deinstallieren. Weitere Informationen finden Sie unter [Lösung aktualisieren](#).

Überblick über die Bereitstellung

Gehen Sie wie folgt vor, um diese Lösung auf zu implementierenAWS.

[\(Optional\) Schritt 0: Starten Sie einen Ticketsystem-Integrationsstapel](#)

- Wenn Sie die Ticketing-Funktion verwenden möchten, stellen Sie zuerst den Ticketing-Integrations-Stack in Ihrem Security Hub-Administratorkonto bereit.
- Kopieren Sie den Namen der Lambda-Funktion aus diesem Stack und stellen Sie ihn als Eingabe für den Admin-Stack bereit (siehe Schritt 1).

[Schritt 1: Starten Sie den Admin-Stack](#)

- Starten Sie die `aws-sharr-deploy.template` AWS CloudFormation Vorlage in Ihrem AWS Security Hub Admin-Konto.
- Wählen Sie aus, welche Sicherheitsstandards installiert werden sollen.
- Wählen Sie eine vorhandene Orchestrator-Protokollgruppe aus, die verwendet werden soll (wählen Sie aus, Yes ob sie `S00111-SHARR-Orchestrator` bereits in einer früheren Installation vorhanden ist).

Schritt 2: Installieren Sie die Behebungsrollen in jedem Mitgliedskonto AWS Security Hub

- Starten Sie die `aws-sharr-member-roles.template` AWS CloudFormation Vorlage in einer Region pro Mitgliedskonto.
- Geben Sie das 12-stellige Konto IG für das AWS Security Hub Administratorkonto ein.

Schritt 3: Starten Sie den Member-Stack

- Geben Sie den Namen der CloudWatch Logs-Gruppe an, die für CIS 3.1-3.14-Korrekturen verwendet werden soll. Es muss der Name einer CloudWatch Logs-Protokollgruppe sein, die Logs empfängt. CloudTrail
- Wählen Sie aus, ob die Behebungsrollen installiert werden sollen. Installieren Sie diese Rollen nur einmal pro Konto.
- Wählen Sie aus, welche Playbooks installiert werden sollen.
- Geben Sie die Konto-ID des AWS Security Hub Administratorkontos ein.

Schritt 4: (Optional) Passen Sie die verfügbaren Abhilfemaßnahmen an

- Entfernen Sie alle Behebungen pro Mitgliedskonto. Dieser Schritt ist optional.

(Optional) Schritt 0: Starten Sie einen Ticketsystem-Integrationsstapel

1. Wenn Sie die Ticketing-Funktion verwenden möchten, starten Sie zuerst den entsprechenden Integrationsstapel.
2. Wählen Sie die bereitgestellten Integrations-Stacks für Jira oder verwenden Sie sie als Vorlage ServiceNow, um Ihre eigene benutzerdefinierte Integration zu implementieren.

So stellen Sie den Jira-Stack bereit:

- a. Geben Sie einen Namen für Ihren Stack ein.
- b. Stellen Sie das URI Ihrer Jira-Instanz zur Verfügung.
- c. Geben Sie den Projektschlüssel für das Jira-Projekt ein, an das Sie Tickets senden möchten.
- d. Erstellen Sie in Secrets Manager ein neues Key-Value-Secret, das Ihre Username Jira und enthält. Password

 Note

Sie können einen API Jira-Schlüssel anstelle Ihres Passworts verwenden, indem Sie Ihren Benutzernamen als Username und Ihren API Schlüssel als angeben. Password

- e. Fügen Sie ARN dieses Geheimnis als Eingabe zum Stack hinzu.

Specify stack details

Provide a stack name

Stack name

Stack name must be 1 to 128 characters, start with a letter, and only contain alphanumeric characters. Character count: 22/128.

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

Jira Project Information

InstanceURI

The URI of your Jira instance. For example: <https://my-jira-instance.atlassian.net>

JiraProjectKey

The key of your Jira project where tickets will be created.

Jira API Credentials

SecretArn

The ARN of the Secrets Manager secret where you have stored your API credentials. This must be a JSON secret with the following keys: Username,Password.

Cancel

Previous

Next

Um den Stack bereitzustellen: ServiceNow

- a. Geben Sie einen Namen für Ihren Stack ein.

Schritt 1: Starten Sie den Admin-Stack

Important

Diese Lösung beinhaltet eine Option zum Senden anonymisierter Betriebsmetriken an AWS. Wir verwenden diese Daten, um besser zu verstehen, wie Kunden diese Lösung und die damit verbundenen Dienstleistungen und Produkte nutzen. AWS besitzt die im Rahmen dieser Umfrage gesammelten Daten. Die Datenerfassung unterliegt der [AWS Datenschutzerklärung](#). Um diese Funktion zu deaktivieren, laden Sie die Vorlage herunter, ändern Sie den AWS CloudFormation Zuordnungsbereich und verwenden Sie dann die AWS CloudFormation Konsole, um Ihre Vorlage hochzuladen und die Lösung bereitzustellen. Weitere Informationen finden Sie im Abschnitt [Anonymisierte Datenerfassung](#) in diesem Leitfaden.

Diese automatisierte AWS CloudFormation Vorlage stellt die automatisierte Sicherheitsreaktion auf AWS einer Lösung in der AWS Cloud bereit. Bevor Sie den Stack starten, müssen Sie Security Hub aktivieren und die [Voraussetzungen erfüllen](#).

Note

Sie sind für die Kosten der AWS Dienste verantwortlich, die Sie beim Betrieb dieser Lösung in Anspruch nehmen. Weitere Informationen finden Sie im Abschnitt [Kosten](#) in diesem Handbuch und auf der Preisseite der einzelnen AWS Dienste, die in dieser Lösung verwendet werden.

1. Melden Sie sich bei AWS Management Console dem Konto an, in dem der aktuell konfiguriert AWS Security Hub ist, und klicken Sie auf die Schaltfläche unten, um die `aws-sharr-deploy.template` AWS CloudFormation Vorlage zu starten.

[Launch solution](#)

Sie können auch [die Vorlage herunterladen](#) als Ausgangspunkt für eine eigene Implementierung verwenden.

2. Die Vorlage wird standardmäßig in der Region USA Ost (Nord-Virginia) gestartet. Um diese Lösung in einer anderen AWS Region zu starten, verwenden Sie die Regionsauswahl in der AWS Management Console Navigationsleiste.

Note

Diese Lösung verwendet AWS Systems Manager, was derzeit nur in bestimmten AWS Regionen verfügbar ist. Die Lösung funktioniert in allen Regionen, die diesen Service unterstützen. Die aktuelle Verfügbarkeit nach Regionen finden Sie in der [Liste der AWS regionalen Dienste](#).

3. Vergewissern Sie sich auf der Seite Stack erstellen, dass sich die richtige Vorlage im Amazon S3 URL S3-Textfeld URL befindet, und wählen Sie dann Weiter.
4. Weisen Sie Ihrem Lösungstapel auf der Seite „Stack-Details angeben“ einen Namen zu. Informationen zu Einschränkungen bei der Benennung von Zeichen finden Sie unter [STSBeschränkungen IAM und Beschränkungen](#) im AWS Identity and Access Management Benutzerhandbuch.
5. Wählen Sie auf der Seite „Parameter“ die Option „Weiter“.

Parameter	Standard	Beschreibung
Laden Sie den SC Admin Stack	yes	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von SC-Steuer-elementen installiert werden sollen.
AFSBPAdmin-Stack laden	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von FSBP Kontrollen installiert werden sollen.
CIS120 Admin-Stack laden	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von CIS120 Kontrollen installiert werden sollen.

Parameter	Standard	Beschreibung
CIS140 Admin-Stack laden	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von CIS140 Kontrollen installiert werden sollen.
Laden Sie CIS300 Admin Stack.	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von CIS300-Steurelementen installiert werden sollen.
PC1321Admin-Stack laden	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von PC1321 Kontrollen installiert werden sollen.
NISTAdmin-Stack laden	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von NIST Kontrollen installiert werden sollen.

Parameter	Standard	Beschreibung
Orchestrator-Protokollgruppe wiederverwenden	no	Wählen Sie aus, ob eine bestehende S00111-SH ARR-Orchestrator CloudWatch Protokollgruppe wiederverwendet werden soll oder nicht. Dies vereinfacht die Neuinstallation und Upgrades, ohne dass Protokolldaten aus einer früheren Version verloren gehen. Wenn Sie ein Upgrade von Version 1.2 oder höher durchführen, wählen Sie. yes
Verwenden Sie Metriken CloudWatch	yes	Geben Sie an, ob CloudWatch Metrics für die Überwachung der Lösung aktiviert werden sollen. Dadurch wird ein CloudWatch Dashboard zum Anzeigen von Metriken erstellt.
Verwenden Sie CloudWatch Metrik-Alarme	yes	Geben Sie an, ob CloudWatch Metrik-Alarme für die Lösung aktiviert werden sollen. Dadurch werden Alarme für bestimmte von der Lösung gesammelte Metriken erstellt.

Parameter	Standard	Beschreibung
RemediationFailureAlarmThreshold	5	<p>Geben Sie den Schwellenwert für den Prozentsatz der Behebungsfehler pro Kontroll-ID an. Wenn Sie beispielsweise einen Wert eingeben 5, erhalten Sie einen Alarm, wenn eine Kontroll-ID an einem bestimmten Tag bei mehr als 5% der Behebungen fehlschlägt.</p> <p>Dieser Parameter funktioniert nur, wenn Alarme erstellt wurden (siehe Parameter „CloudWatch Metrik-Alarme verwenden“).</p>
EnableEnhancedCloudWatchMetrics	no	<p>Wenn <code>yes</code>, werden zusätzliche CloudWatch Messwerte erstellt, um die gesamte Steuerung IDs einzeln auf dem CloudWatch Dashboard und als CloudWatch Alarme nachzuverfolgen.</p> <p>Informationen zu den zusätzlichen Kosten, die dadurch entstehen, finden Sie im Abschnitt Kosten.</p>

Parameter	Standard	Beschreibung
TicketGenFunctionName	(Optionale Eingabe)	Optional. Lassen Sie das Feld leer, wenn Sie kein Ticketsystem integrieren möchten. Andernfalls geben Sie den Lambda-Funktionsnamen aus der Stack-Ausgabe von Schritt 0 an, zum Beispiel: <code>S00111-ASR-ServiceNow-TicketGenerator</code> .

- Wählen Sie auf der Seite Configure stack options (Stack-Optionen konfigurieren) Next (Weiter) aus.
- Überprüfen und bestätigen Sie die Einstellungen auf der Seite Review. Markieren Sie das Kästchen, um zu bestätigen, dass die Vorlage Ressourcen AWS Identity and Access Management (IAM) erstellt.
- Wählen Sie Stack erstellen aus, um den Stack bereitzustellen.

Sie können den Status des Stacks in der AWS CloudFormation Konsole in der Spalte Status einsehen. Sie sollten in etwa 15 Minuten COMPLETE den Status CREATE _ erhalten.

Schritt 2: Installieren Sie die Behebungsrollen in jedem AWS Security Hub-Mitgliedskonto

Die `aws-sharr-member-roles.template` StackSet dürfen nur in einer Region pro Mitgliedskonto bereitgestellt werden. Es definiert die globalen Rollen, die kontenübergreifende API Aufrufe von der SHARR Orchestrator-Step-Funktion aus ermöglichen.

- Melden Sie sich für jedes AWS Security Hub Mitgliedskonto (einschließlich des Administratorkontos, das ebenfalls Mitglied ist) bei der AWS Management Console an. Wählen Sie die Schaltfläche, um die `aws-sharr-member-roles.template` AWS CloudFormation Vorlage zu starten. Sie können auch [die Vorlage herunterladen](#) als Ausgangspunkt für eine eigene Implementierung verwenden.

2. Die Vorlage wird standardmäßig in der Region USA Ost (Nord-Virginia) gestartet. Um diese Lösung in einer anderen AWS Region zu starten, verwenden Sie die Regionsauswahl in der Navigationsleiste der AWS Management Console.
3. Vergewissern Sie sich auf der Seite Stack erstellen, dass sich die richtige Vorlage im Amazon S3 URL S3-Textfeld URL befindet, und wählen Sie dann Weiter.
4. Weisen Sie Ihrem Lösungstapel auf der Seite „Stack-Details angeben“ einen Namen zu. Informationen zu Einschränkungen bei der Benennung von Zeichen finden Sie unter IAM und STS Beschränkungen im AWS Identity and Access Management-Benutzerhandbuch.
5. Geben Sie auf der Seite Parameter die folgenden Parameter an und klicken Sie auf Weiter.

Parameter	Standard	Beschreibung
Namespace	<i><Requires input></i>	Geben Sie eine Zeichenfolge mit bis zu 9 alphanumerischen Kleinbuchstaben ein. Diese Zeichenfolge wird Teil der IAM Rollennamen. Verwenden Sie denselben Wert für die Bereitstellung des Mitgliedsstapels und die Bereitstellung des Stacks für Mitgliedsrollen.
Sec Hub-Kontoadministrator	<i><Requires input></i>	Geben Sie die 12-stellige Konto-ID für das AWS Security Hub Administratorkonto ein. Dieser Wert gewährt der Lösungsrolle des Administratorkontos Berechtigungen.

6. Wählen Sie auf der Seite Configure stack options (Stack-Optionen konfigurieren) Next (Weiter) aus.

- Überprüfen und bestätigen Sie die Einstellungen auf der Seite Review. Markieren Sie das Kästchen, um zu bestätigen, dass die Vorlage Ressourcen AWS Identity and Access Management (IAM) erstellt.
- Wählen Sie Stack erstellen aus, um den Stack bereitzustellen.

Sie können den Status des Stacks in der AWS CloudFormation Konsole in der Spalte Status einsehen. Sie sollten in etwa 5 Minuten COMPLETE den Status CREATE _ erhalten. Sie können mit dem nächsten Schritt fortfahren, während dieser Stapel geladen wird.

Schritt 3: Starten Sie den Member-Stack

Important

Diese Lösung beinhaltet eine Option zum Senden anonymisierter Betriebsmetriken an AWS. Wir verwenden diese Daten, um besser zu verstehen, wie Kunden diese Lösung und die damit verbundenen Dienstleistungen und Produkte nutzen. AWS besitzt die im Rahmen dieser Umfrage gesammelten Daten. Die Datenerfassung unterliegt den AWS Datenschutzbestimmungen.

Um diese Funktion zu deaktivieren, laden Sie die Vorlage herunter, ändern Sie den AWS CloudFormation Zuordnungsbereich und verwenden Sie dann die AWS CloudFormation Konsole, um Ihre Vorlage hochzuladen und die Lösung bereitzustellen. Weitere Informationen finden Sie im Abschnitt [Erfassung von Betriebskennzahlen](#) in diesem Leitfaden.

Der `aws-sharr-member` Stack muss in jedem Security Hub-Mitgliedskonto installiert werden. Dieser Stack definiert die Runbooks für die automatisierte Problembehebung. Der Administrator jedes Mitgliedskontos kann kontrollieren, welche Abhilfemaßnahmen über diesen Stack verfügbar sind.

- Melden Sie sich AWS Management Console für jedes AWS Security Hub Mitgliedskonto an (einschließlich des Administratorkontos, das ebenfalls Mitglied ist). Wählen Sie die Schaltfläche, um die `aws-sharr-member.template` AWS CloudFormation Vorlage zu starten.

[Launch solution](#)

Sie können auch [die Vorlage herunterladen](#) als Ausgangspunkt für eine eigene Implementierung verwenden.

- Die Vorlage wird standardmäßig in der Region USA Ost (Nord-Virginia) gestartet. Um diese Lösung in einer anderen AWS Region zu starten, verwenden Sie die Regionsauswahl in der AWS Management Console Navigationsleiste.

 Note

Diese Lösung verwendet AWS Systems Manager, was derzeit in den meisten AWS Regionen verfügbar ist. Die Lösung funktioniert in allen Regionen, die diese Dienste unterstützen. Die aktuelle Verfügbarkeit nach Regionen finden Sie in der [Liste der AWS regionalen Dienste](#).

- Vergewissern Sie sich auf der Seite Stack erstellen, dass sich die richtige Vorlage im Amazon S3 URL S3-Textfeld URL befindet, und wählen Sie dann Weiter.
- Weisen Sie Ihrem Lösungsstapel auf der Seite „Stack-Details angeben“ einen Namen zu. Informationen zu Einschränkungen bei der Benennung von Zeichen finden Sie unter [STSBeschränkungen IAM und Beschränkungen](#) im AWS Identity and Access Management Benutzerhandbuch.
- Geben Sie auf der Seite „Parameter“ die folgenden Parameter an und klicken Sie auf Weiter.

Parameter	Standard	Beschreibung
Geben Sie den Namen der LogGroup an, die zur Erstellung von metrischen Filtern und Alarmen verwendet werden sollen	<i><Requires input></i>	Geben Sie den Namen einer CloudWatch Logs-Gruppe an, in der API Aufrufe CloudTrail protokolliert werden. Dies wird für CIS 3.1-3.14-Korrekturen verwendet.
Laden Sie den SC-Mitgliedsstapel	yes	Geben Sie an, ob die Mitgliedskomponenten für die automatische Wiederherstellung der SC-Steuer elemente installiert werden sollen.

Parameter	Standard	Beschreibung
AFSBPMitgliedsstapel laden	no	Geben Sie an, ob die Mitgliedskomponenten für die automatische Korrektur von FSBP Kontrollen installiert werden sollen.
Stapel mit CIS12 0 Mitgliedern laden	no	Geben Sie an, ob die Mitgliedskomponenten für die automatische Korrektur von CIS12 0 Kontrollen installiert werden sollen.
Stapel mit CIS14 0 Mitgliedern laden	no	Geben Sie an, ob die Mitgliedskomponenten für die automatische Korrektur von CIS14 0 Kontrollen installiert werden sollen.
Laden Sie den Stapel mit CIS3 00 Mitgliedern	no	Geben Sie an, ob die Mitgliedskomponenten für die automatische Korrektur von CIS3 00-Steurelementen installiert werden sollen.
PC1321Mitgliedsstapel laden	no	Geben Sie an, ob die Mitgliedskomponenten für die automatische Korrektur von PC1321 Kontrollen installiert werden sollen.
NISTMitgliedsstapel laden	no	Geben Sie an, ob die Mitgliedskomponenten für die automatische Korrektur von NIST Kontrollen installiert werden sollen.

Parameter	Standard	Beschreibung
S3-Bucket für Redshift Audit Logging erstellen	no	Wählen Sie ausyes, ob der S3-Bucket für die FSBP RedShift 4.4-Problemebehebung erstellt werden soll. Einzelheiten zum S3-Bucket und zur Behebung finden Sie unter Redshift. 4-Problemebehebung im Benutzerhandbuch.AWS Security Hub
Sec Hub-Administratorkonto	<i><Requires input></i>	Geben Sie die 12-stellige Konto-ID für das AWS Security Hub-Administratorkonto ein.
Namespace	<i><Requires input></i>	Geben Sie eine Zeichenfolge mit bis zu 9 alphanumerischen Kleinbuchstaben ein. Diese Zeichenfolge wird Teil der IAM Rollennamen und des Action Log S3-Buckets. Verwenden Sie denselben Wert für die Bereitstellung des Member-Stacks und die Stack-Bereitstellung der Mitgliedsrollen. Diese Zeichenfolge muss den Amazon S3 S3-Benennungsregeln für allgemeine S3-Buckets entsprechen.

Parameter	Standard	Beschreibung
EnableCloudTrailForASRActionLog	no	Wählen Sie im CloudWatch Dashboard aus, yes ob Sie die von der Lösung durchgeführten Verwaltungsgereignisse überwachen möchten. Die Lösung erstellt in jedem Mitgliedskonto, das Sie auswählen, eine CloudTrail Spurensammlung, die Informationen zu den zusätzlichen Kosten , die dadurch entstehen, finden Sie im Abschnitt Kosten.

- Wählen Sie auf der Seite Configure stack options (Stack-Optionen konfigurieren) Next (Weiter) aus.
- Überprüfen und bestätigen Sie die Einstellungen auf der Seite Review. Markieren Sie das Kästchen, um zu bestätigen, dass die Vorlage Ressourcen AWS Identity and Access Management (IAM) erstellt.
- Wählen Sie Stack erstellen aus, um den Stack bereitzustellen.

Sie können den Status des Stacks in der AWS CloudFormation Konsole in der Spalte Status einsehen. Sie sollten in etwa 15 Minuten COMPLETE den Status CREATE _ erhalten.

Schritt 4: (Optional) Passen Sie die verfügbaren Abhilfemaßnahmen an

Wenn Sie bestimmte Abhilfemaßnahmen aus einem Mitgliedskonto entfernen möchten, können Sie dies tun, indem Sie den verschachtelten Stack entsprechend dem Sicherheitsstandard aktualisieren. Der Einfachheit halber werden die Optionen für verschachtelte Stacks nicht an den Root-Stack weitergegeben.

- Melden Sie sich bei der [AWS CloudFormation Konsole](#) an und wählen Sie den verschachtelten Stack aus.
- Wählen Sie Aktualisieren.
- Wählen Sie Verschachtelten Stack aktualisieren und dann Stack aktualisieren aus.

Update sharr-v130-rc1-member-PlaybookMemberStackPCI321-LWXPIU3B3J89? ✕

It is recommended to update through the root stack
Updating a nested stack may result in an unstable state where the nested stack is out-of-sync with its root stack. [Learn more](#)

Go to root stack (recommended)

Update nested stack

Cancel Update stack

Verschachtelten Stapel aktualisieren

4. Wählen Sie Aktuelle Vorlage verwenden und dann Weiter aus.
5. Passen Sie die verfügbaren Abhilfemaßnahmen an. Ändern Sie die Werte für gewünschte Kontrollen auf Available und für unerwünschte Kontrollen auf. Not available

Note

Wenn Sie eine Problembehebung deaktivieren, wird das Runbook zur Problembehebung für den Sicherheitsstandard und die Sicherheitskontrolle entfernt.

6. Wählen Sie auf der Seite Configure stack options (Stack-Optionen konfigurieren) Next (Weiter) aus.
7. Überprüfen und bestätigen Sie die Einstellungen auf der Seite Review. Markieren Sie das Kästchen, um zu bestätigen, dass die Vorlage Ressourcen () erstellt AWS Identity and Access Management . IAM
8. Wählen Sie Stack aktualisieren aus.

Sie können den Status des Stacks in der AWS CloudFormation Konsole in der Spalte Status einsehen. Sie sollten in etwa 15 Minuten COMPLETE den Status CREATE _ erhalten.

Überwachen Sie die Lösung mit Service Catalog AppRegistry

Diese Lösung umfasst eine Service AppRegistry Catalog-Ressource, mit der die CloudFormation Vorlage und die zugrunde liegenden Ressourcen als Anwendung sowohl in [Service Catalog AppRegistry](#) als auch im [AWS Systems Manager Application Manager](#) registriert werden können.

AWS Systems Manager Application Manager bietet Ihnen einen Überblick über diese Lösung und ihre Ressourcen auf Anwendungsebene, sodass Sie:

- Überwachen Sie die Ressourcen, die Kosten für die bereitgestellten Ressourcen über Stacks und AWS-Konten die mit dieser Lösung verknüpften Protokolle von einem zentralen Standort aus.
- Zeigen Sie Betriebsdaten für die Ressourcen dieser Lösung (z. B. Bereitstellungsstatus, CloudWatch Alarmer, Ressourcenkonfigurationen und Betriebsprobleme) im Kontext einer Anwendung an.

Die folgende Abbildung zeigt ein Beispiel für die Anwendungsansicht für den Lösungstapel in Application Manager.

The screenshot displays the AWS Systems Manager Application Manager interface. On the left, a sidebar shows a tree view under 'Components (2)' with 'AWS-Systems-Manager-A' selected. The main content area is titled 'AWS-Systems-Manager-Application-Manager' and includes a 'Start runbook' button. Below the title is the 'Application information' section, which contains a 'View in AppRegistry' button and details such as 'Application type: AWS-AppRegistry', 'Name: AWS-Systems-Manager-Application-Manager', and 'Application monitoring: Not enabled'. A description states: 'Service Catalog application to track and manage all your resources for the solution'. A navigation bar below this section includes tabs for Overview, Resources, Instances, Compliance, Monitoring, OpsItems, Logs, Runbooks, and Cost. At the bottom, there are two summary cards: 'Insights and Alarms' with a 'View all' button and 'Cost' with a 'View all' button. The cost card shows 'Cost (USD)' with a value of '-'. A 'Start runbook' button is also visible in the top right corner.

Lösungstapel im Anwendungsmanager

Verwenden Sie CloudWatch Application Insights

Diese Lösung lässt sich bei der Bereitstellung automatisch in CloudWatch Application Insights integrieren. CloudWatch Application Insights hilft Ihnen, den Zustand und die Leistung der Lösung zu erkennen und zu verstehen, und zwar durch:

- Automatische Erkennung und Überwachung wichtiger Anwendungsressourcen.
- Erstellung benutzerdefinierter Alarme zur proaktiven Identifizierung potenzieller Probleme.
- Automatisches Generieren des Systems Manager OpsItems , wenn Anomalien oder Ausfälle erkannt werden. Diese OpsItems dienen als umsetzbare Benachrichtigungen, die Sie umgehend über Probleme informieren, die sich auf die Lösung auswirken.

Gehen Sie wie folgt vor, um das CloudWatch Application Insights-Überwachungs-Dashboard aufzurufen, in dem Sie den Zustand der Lösung überprüfen und wichtige Komponenten anhand vorkonfigurierter Dashboards und Alarme überwachen können.

1. Navigieren Sie zur [CloudWatch -Konsole](#).
2. Wählen Sie die Registerkarte Insights und anschließend Application Insights aus.
3. Wählen Sie die Registerkarte Anwendungen und dann die der Lösung zugeordnete Anwendung aus.

Sie können auch das CloudWatch Dashboard der Lösung importieren, um Ihre Überwachung des Zustands der Lösung zu konsolidieren. Gehen Sie im Anwendungs-Dashboard der Lösung in CloudWatch Application Insights wie folgt vor:

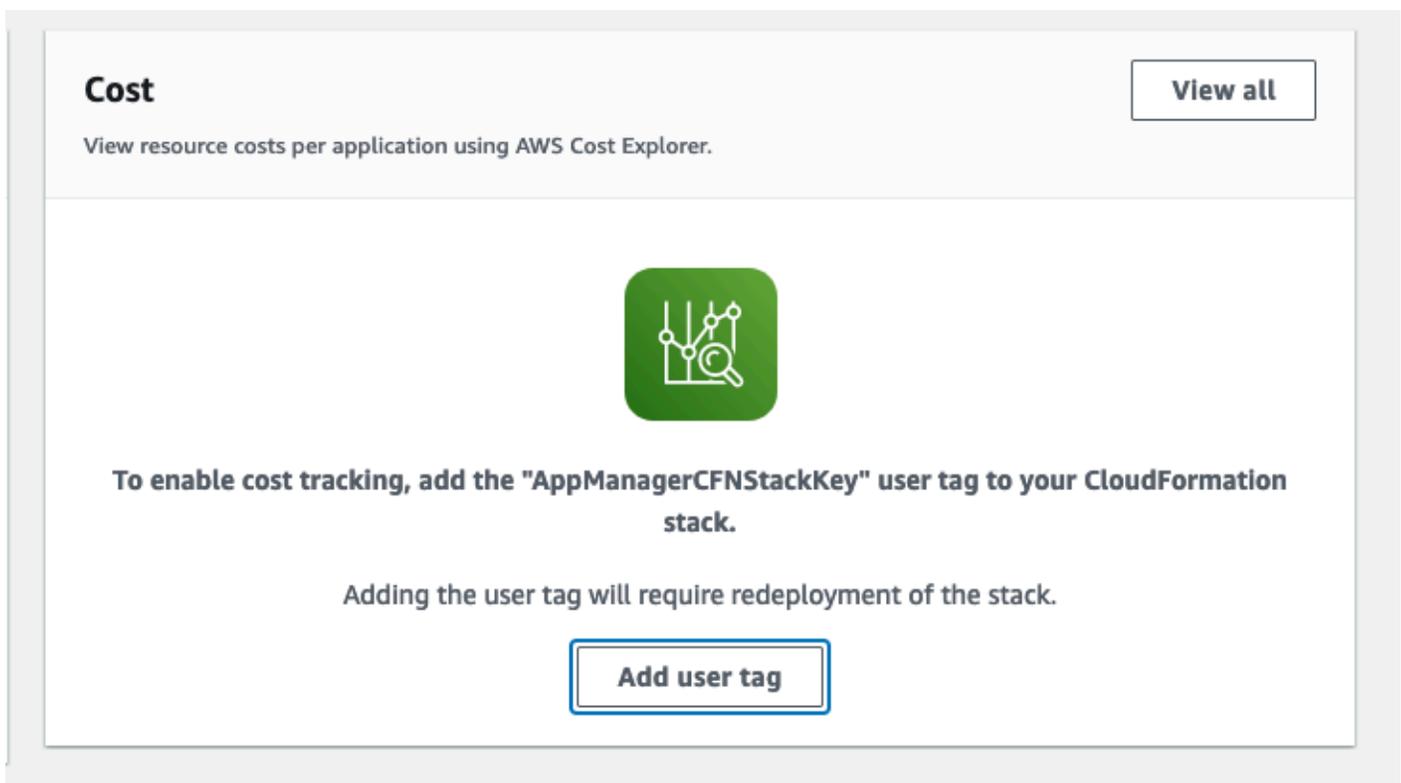
1. Wählen Sie die Registerkarte Benutzerdefiniertes CloudWatch Dashboard.
2. Wählen Sie „CloudWatch Dashboard importieren“.
3. Geben Sie ASR-Remediation-Metrics-Dashboard in das Suchfeld die automatische Sicherheitsantwort ein und wählen Sie sie im AWS Dashboard aus.
4. Wählen Sie Importieren aus.

Jetzt können Sie das CloudWatch Application Insights-Dashboard und das benutzerdefinierte Dashboard der Lösung sowohl in der CloudWatch Application Insights-Konsole anzeigen, ohne zwischen den Seiten wechseln zu müssen.

Bestätigen Sie die mit der Lösung verknüpften Kostenangaben

Nachdem Sie die mit der Lösung verknüpften Kostenzuordnungs-Tags aktiviert haben, müssen Sie die Kostenzuordnungs-Tags bestätigen, um die Kosten für diese Lösung zu sehen. So bestätigen Sie die Tags für die Kostenzuweisung:

1. Melden Sie sich bei der [Systems Manager Manager-Konsole](#) an.
2. Wählen Sie im Navigationsbereich Application Manager aus.
3. Wählen Sie unter Anwendungen den Anwendungsnamen für diese Lösung und wählen Sie ihn aus.
4. Wählen Sie auf der Registerkarte Übersicht unter Kosten die Option Benutzertag hinzufügen aus.



5. Geben Sie auf der Seite „Benutzertag hinzufügen“ den Text ein `confirm` und wählen Sie dann Benutzertag hinzufügen aus.

Es kann bis zu 24 Stunden dauern, bis der Aktivierungsvorgang abgeschlossen ist und die Tag-Daten angezeigt werden.

Aktivieren Sie die mit der Lösung verknüpften Kostenzuweisungs-Tags

Nachdem Sie die mit dieser Lösung verknüpften Kosten-Tags bestätigt haben, müssen Sie die Kostenzuweisungs-Tags aktivieren, um die Kosten für diese Lösung zu sehen. Die Kostenzuweisungs-Tags können nur über das Verwaltungskonto der Organisation aktiviert werden.

So aktivieren Sie Tags für die Kostenzuweisung:

1. Melden Sie sich bei der [AWS Billing and Cost Management und Cost Management Console](#) an.
2. Wählen Sie im Navigationsbereich die Option Cost Allocation Tags aus.
3. Filtern Sie auf der Seite mit den Tags für die Kostenzuweisung AppManagerCFNStackKey nach dem Tag und wählen Sie dann das Tag aus den angezeigten Ergebnissen aus.
4. Wählen Sie Activate.

AWS Cost Explorer

Durch die Integration mit Cost Explorer können Sie sich in der Application Manager-Konsole einen Überblick über die mit der Anwendung und den Anwendungskomponenten verbundenen AWS Kosten anzeigen lassen. Der Cost Explorer hilft Ihnen bei der Kostenverwaltung, indem er Ihnen einen Überblick über Ihre AWS Ressourcenkosten und -nutzung im Laufe der Zeit bietet.

1. Melden Sie sich bei der [AWS Cost Management Console](#) an.
2. Wählen Sie im Navigationsmenü Cost Explorer aus, um die Kosten und die Nutzung der Lösung im Laufe der Zeit anzuzeigen.

Überwachen Sie den Betrieb der Lösung mit einem CloudWatch Amazon-Dashboard

Diese Lösung umfasst benutzerdefinierte Metriken und Alarme, die auf einem CloudWatch Amazon-Dashboard angezeigt werden.

Das CloudWatch Dashboard und die Alarme überwachen den Betrieb der Lösung und warnen, wenn ein potenzielles Problem auftritt.

Aktivierung von CloudWatch Metriken, Alarmen und Dashboards

Es gibt vier CloudFormation Vorlagenparameter für die CloudWatch Funktionalität.

The screenshot shows a section titled "CloudWatch Metrics" with four parameters:

- UseCloudWatchMetrics**: Enable collection of operational metrics and create a CloudWatch dashboard to monitor solution operations. Value: yes.
- UseCloudWatchMetricsAlarms**: Create CloudWatch Alarms for gathered metrics. Value: yes.
- RemediationFailureAlarmThreshold**: Percentage of failures in one period (default period is 1 day) to trigger the remediation failures alarm for a given control ID. E.g., to specify 20% then enter the number 20. Value: 5.
- EnableEnhancedCloudWatchMetrics**: Enable collection of metrics per Control ID in addition to standard metrics. You must also select 'yes' for UseCloudWatchMetrics to enable enhanced metric collection. The added cost of these additional custom metrics could be up to \$65/month. Value: no.

1. **UseCloudWatchMetrics**— Diese Einstellung `yes` ermöglicht die Erfassung von Betriebskennzahlen und erstellt ein CloudWatch Dashboard, in dem diese Kennzahlen angezeigt werden.
2. **UseCloudWatchAlarms**— Wenn Sie diese Einstellung auf `yes` einstellen, werden die Standardalarme der Lösung `yes` aktiviert.
3. **RemediationFailureAlarmThreshold**— Der Prozentsatz fehlgeschlagener Problembehebungen in einem Zeitraum, in dem ein Alarm ausgelöst wurde.
4. **EnableEnhancedCloudWatchMetrics**— Stellen Sie diesen Parameter auf `yes` ein, um einzelne Metriken pro Kontroll-ID zu sammeln. Standardmäßig ist dieser Parameter auf `no` gesetzt, sodass nur Metriken zur Gesamtzahl der Behebungen in allen Kontrollen erfasst werden. Für einzelne Metriken und Alarme pro Kontroll-ID fallen zusätzliche Kosten an.

Verwenden des Dashboards CloudWatch

So zeigen Sie das Dashboard an:

1. Navigieren Sie zu Amazon CloudWatch und dann zu Dashboards.
2. Wählen Sie das Dashboard mit dem Namen "ASR-Remediation-Metrics-Dashboard" aus.

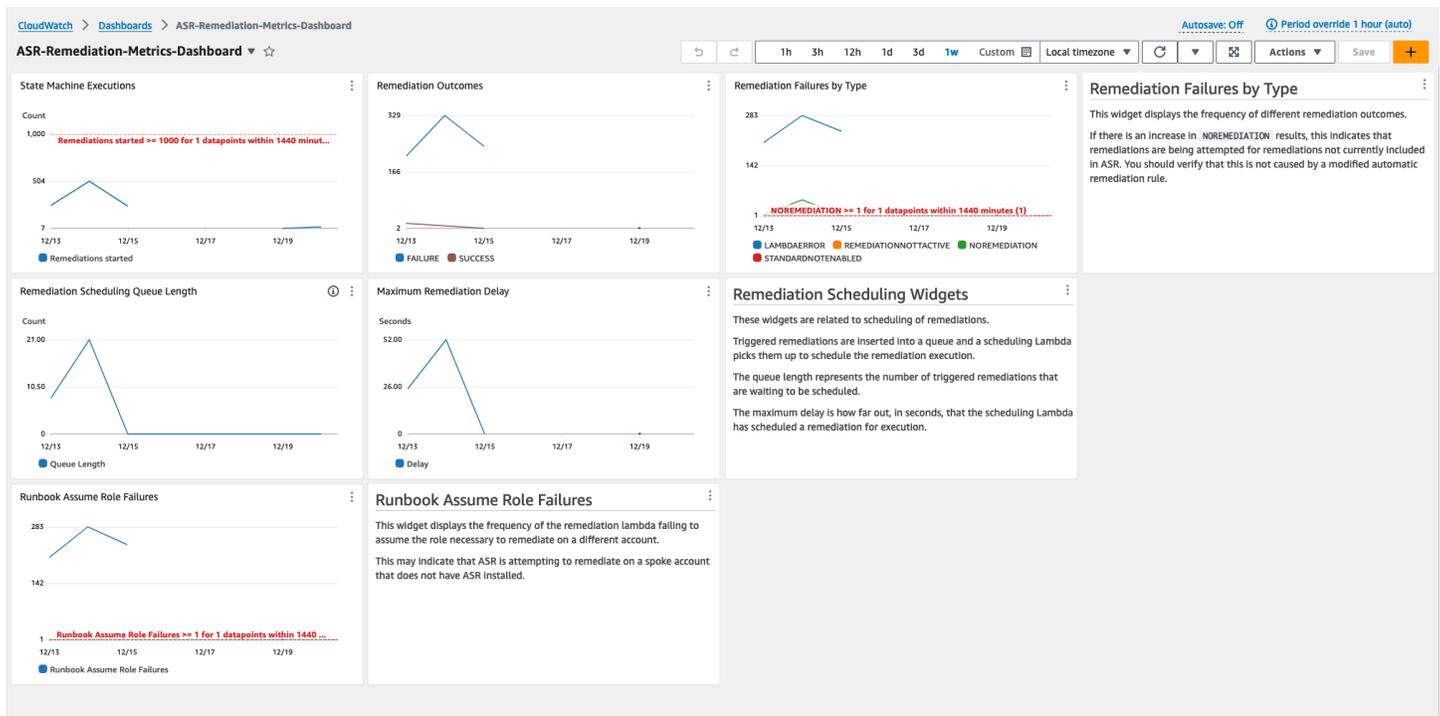
Das CloudWatch Dashboard enthält die folgenden Abschnitte:

1. Erfolgreiche Problembehebungen insgesamt — Gibt Ihnen einen Einblick in die Anzahl der Security Hub Hub-Ergebnisse, die durch die Lösung erfolgreich behoben wurden.
2. Behebungsfehler — Zeigt an, wie viele Behebungen insgesamt und als Prozentsatz fehlgeschlagen sind, sowie die Fehlerursache. Eine hohe Anzahl von Ausfällen kann auf ein technisches Problem mit der Lösung hinweisen, das Sie möglicherweise genauer untersuchen müssen.
3. Behebung erfolgreich/fehlgeschlagen nach Kontroll-ID — Wenn Sie bei der Bereitstellung die Option Erweiterte Metriken aktiviert haben, werden in diesem Abschnitt die Behebungsergebnisse nach Kontroll-ID aufgelistet. Wenn im Abschnitt „Behebungsfehler“ generell eine hohe Ausfallrate angezeigt wird, wird in diesem Abschnitt angezeigt, ob die Fehler auf viele IDs Steuerungen verteilt sind oder ob nur bestimmte Kontrollen ausfallen. IDs
4. Runbook Assume Role Failures — Zeigt die Anzahl der Fehler an, die aufgrund von Behebungsversuchen in Konten aufgetreten sind, auf denen die Rolle „Lösungsmitglied“ nicht installiert ist. Wiederholte Fehler aufgrund automatisierter Behebungsversuche aufgrund fehlender Rollen verursachen unnötige Kosten. Vermeiden Sie dies, indem Sie den [Mitgliederrollenstapel](#) in den betroffenen Konten installieren, [alle von der Lösung erstellten EventBridge Regeln deaktivieren](#) oder die [Zuordnung des Kontos](#) in Security Hub aufheben.
5. Cloud Trail Management-Aktionen von ASR — Führt die Verwaltungsaktionen der Lösung für alle Mitgliedskonten auf, für die Sie zum Zeitpunkt der Bereitstellung die Aktionsprotokolle mit dem EnableCloudTrailForASRActionLogParameter aktiviert haben. Wenn Sie unerwartete Ressourcenänderungen in einem Ihrer AWS Konten beobachten, können Sie anhand dieses Widgets nachvollziehen, ob Ressourcen durch die Lösung geändert wurden.

Das CloudWatch Dashboard verfügt außerdem über vordefinierte Alarme, die auf häufig auftretende Betriebsfehler hinweisen.

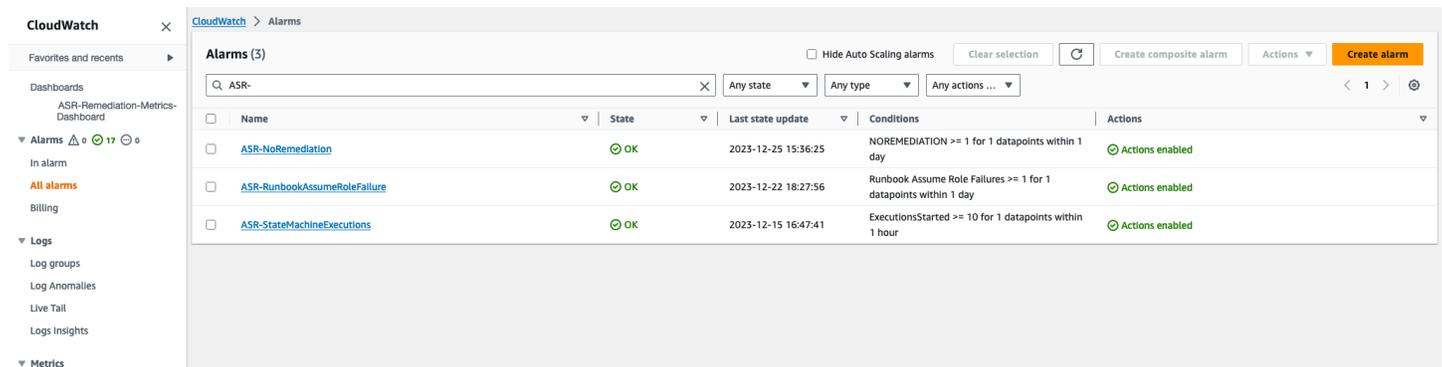
1. State Machine-Ausführungen > 1000 innerhalb von 24 Stunden.
 - a. Ein starker Anstieg der Behebungsausführungen könnte darauf hindeuten, dass eine Ereignisregel häufiger als beabsichtigt initiiert wird.
 - b. Der Schwellenwert kann mithilfe des Parameters geändert werden. CloudFormation
2. Behebungsfehler nach Typ = NOREMEDIATION > 0
 - a. Es werden Korrekturmaßnahmen für Korrekturen versucht, die nicht in enthalten sind. ASR Dies könnte darauf hindeuten, dass eine Ereignisregel so geändert wurde, dass sie mehr als die vorgesehenen Behebungen umfasst.
3. Runbook Assume Role: Fehler > 0
 - a. Gegenmaßnahmen werden für Konten oder Regionen versucht, in denen die Lösung nicht ordnungsgemäß bereitgestellt wurde. Dies könnte darauf hindeuten, dass eine Ereignisregel so geändert wurde, dass sie mehr Konten als beabsichtigt umfasst.

Alle Alarmschwellenwerte können an die individuellen Einsatzanforderungen angepasst werden.



Änderung der Alarmschwellenwerte

1. Navigieren Sie zu Amazon CloudWatch -> Alarms -> All Alarms.
2. Wählen Sie den Alarm aus, den Sie ändern möchten, und wählen Sie dann Aktionen -> Bearbeiten.



The screenshot shows the AWS CloudWatch Alarms console. The left sidebar contains navigation options: Dashboards, Favorites and recents, Alarms (17), In alarm, All alarms, Billing, Logs, Log groups, Log Anomalies, Live Tail, Logs Insights, and Metrics. The main content area displays a table of 3 alarms, all in an 'OK' state. The table columns are Name, State, Last state update, Conditions, and Actions.

Name	State	Last state update	Conditions	Actions
ASR-NoRemediation	OK	2023-12-25 15:36:25	NOREMEDIATION >= 1 for 1 datapoints within 1 day	Actions enabled
ASR-RunbookAssumeRoleFailure	OK	2023-12-22 18:27:56	Runbook Assume Role Failures >= 1 for 1 datapoints within 1 day	Actions enabled
ASR-StateMachineExecutions	OK	2023-12-15 16:47:41	ExecutionsStarted >= 10 for 1 datapoints within 1 hour	Actions enabled

3. Ändern Sie den Schwellenwert auf den gewünschten Wert und speichern Sie.

CloudWatch > Alarms > ASR-StateMachineExecutions > Edit

Step 1 - optional
Specify metric and conditions

Step 2 - optional
[Configure actions](#)

Step 3 - optional
[Add name and description](#)

Step 4 - optional
[Preview and create](#)

Specify metric and conditions - optional

Edit

Metric

Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 day.

Count

1,000

501

1

01/05 01/07 01/09 01/11

ExecutionsStarted

Namespace
AWS/States

Metric name

StateMachineArn

Statistic

Period

Conditions

Threshold type

Static
Use a value as a threshold

Anomaly detection
Use a band as a threshold

Whenever ExecutionsStarted is...

Define the alarm condition.

Greater
> threshold

Greater/Equal
>= threshold

Lower/Equal
<= threshold

Lower
< threshold

than...

Define the threshold value.

Must be a number

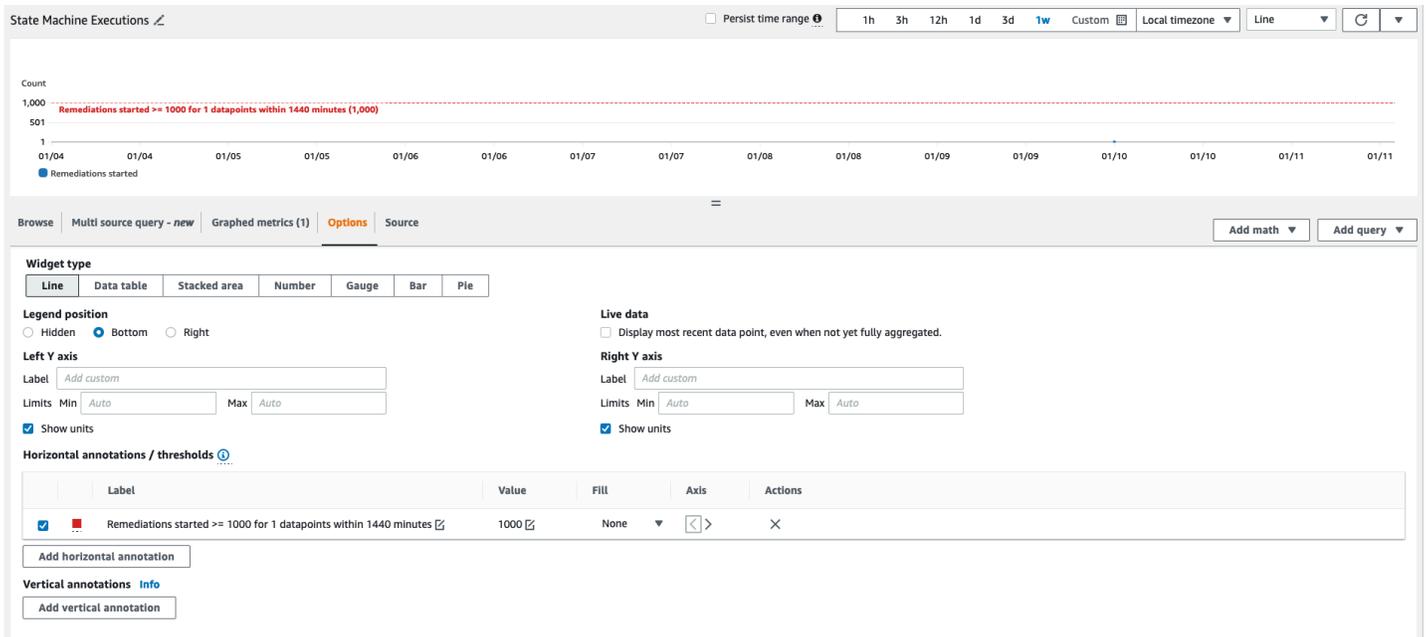
▶ Additional configuration

Cancel
Skip to Preview and create
Next

4. Navigieren Sie zum CloudWatch Dashboard, um die dortigen Diagramme an die neuen Einstellungen anzupassen.

a. Wählen Sie die Ellipse oben rechts im entsprechenden Widget aus.

- b. Wählen Sie Bearbeiten aus.
- c. Wechseln Sie zur Registerkarte Optionen.
- d. Passen Sie die Alarmanmerkung an die neuen Einstellungen an.



Alarmbenachrichtigungen abonnieren

Abonnieren Sie im Administratorkonto das vom Admin-Stack erstellte SNS Amazon-Thema SO0111-ASR_Alarm_Topic. Dadurch werden Sie benachrichtigt, wenn ein Alarm den Status erreicht. ALARM

Aktualisieren Sie die Lösung

Aktualisierung von Versionen vor v1.4

Wenn Sie die Lösung bereits vor Version 1.4.x bereitgestellt haben, deinstallieren Sie sie und installieren Sie dann die neueste Version:

1. Deinstallieren Sie die zuvor bereitgestellte Lösung. Weitere Informationen finden Sie [unter Lösung deinstallieren](#).
2. Starten Sie die neueste Vorlage. Weitere Informationen finden Sie [unter Lösung bereitstellen](#).

Note

Wenn Sie ein Upgrade von Version 2.1 oder früher auf Version 3.0 oder höher durchführen, setzen Sie die Option Vorhandene Orchestrator-Protokollgruppe verwenden auf. No Wenn Sie Version 1.3.0 oder höher neu installieren, können Sie diese Option auswählen. Yes Mit dieser Option können Sie weiterhin bei derselben Protokollgruppe für die Orchestrator-Step-Funktionen protokollieren.

Aktualisierung von Version 1.4 und höher

Wenn Sie ein Upgrade von Version 1.4.x durchführen, aktualisieren Sie alle Stacks oder wie folgt: StackSets

1. Aktualisieren Sie den Stack im Security Hub-Administratorkonto mit der [neuesten Vorlage](#).
2. Aktualisieren Sie in jedem Mitgliedskonto die Berechtigungen aus der neuesten Vorlage.
3. Aktualisieren Sie in jedem Mitgliedskonto in allen Regionen, in denen es derzeit bereitgestellt wird, den Mitgliederstapel anhand der neuesten Vorlage.

Upgrade von v2.0.x

Wenn Sie ein Upgrade von v2.0.x durchführen, führen Sie ein Upgrade auf v2.1.2 oder höher durch. Die Aktualisierung auf v2.1.0 - v2.1.1 schlägt fehl. CloudFormation

Fehlerbehebung

Die [Lösung bekannter Probleme](#) enthält Anweisungen zur Behebung bekannter Fehler. Wenn diese Anweisungen Ihr Problem nicht lösen, erhalten Sie von [Contact AWS Support](#) Anweisungen zum Öffnen einer AWS Support-Anfrage für diese Lösung.

Lösungsprotokolle

Dieser Abschnitt enthält Informationen zur Fehlerbehebung für diese Lösung. Themen finden Sie in der linken Navigationsleiste.

Diese Lösung sammelt die Ergebnisse aus den Behebungs-Runbooks, die unter ausgeführt werden AWS Systems Manager, und protokolliert die Ergebnisse in der Gruppe CloudWatch Logs S00111-SHARR im AWS Security Hub Administratorkonto. Pro Steuerung und Tag gibt es einen Stream.

Die Orchestrator-Schrittfunktionen protokollieren alle Schrittübergänge in der S00111-SHARR-Orchestrator CloudWatch Protokollgruppe im AWS Security Hub-Administratorkonto.

Dieses Protokoll ist ein Audit-Trail, um Zustandsübergänge für jede Instanz der Step Functions aufzuzeichnen. Pro Ausführung von Step Functions gibt es einen Protokollstream.

Beide Protokollgruppen werden mit einem AWS KMS Customer-Manager-Schlüssel (CMK) verschlüsselt.

Die folgenden Informationen zur Fehlerbehebung verwenden die S00111-SHARR Protokollgruppe. Verwenden Sie dieses Protokoll sowie die AWS Systems Manager Automation-Konsole, Automation Executions-Protokolle, die Step Function-Konsole und Lambda-Protokolle, um Probleme zu beheben.

Schlägt eine Problembhebung fehl, wird eine Meldung ähnlich der folgenden S00111-SHARR im Log-Stream für Standard, Kontrolle und Datum protokolliert. Zum Beispiel: CIS -2.9-2021-08-12

```
ERROR: a4cbb9bb-24cc-492b-a30f-1123b407a6253: Remediation failed for CIS control
2.9 in account 123412341234: See Automation Execution output for details (AwsEc2Vpc
vpc-0e92bbe911cf08acb)
```

Die folgenden Meldungen enthalten zusätzliche Informationen. Diese Ausgabe stammt aus dem SHARR Runbook für den Sicherheitsstandard und die Kontrolle. Zum Beispiel: SHARR- CIS _1.2.0_2.9

```
Step fails when it is Execution complete: verified. Failed to run automation with executionId: eecdef79-9111-4532-921a-e098549f5259 Failed : {Status=[Failed], Output=[No output available yet because the step is not successfully executed], ExecutionId=[eecdef79-9111-4532-921a-e098549f5259]}. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.
```

Diese Information weist Sie auf den Fehler hin, bei dem es sich in diesem Fall um eine untergeordnete Automatisierung handelte, die im Mitgliedskonto ausgeführt wurde. Um dieses Problem zu beheben, müssen Sie sich AWS Management Console im Mitgliedskonto anmelden (aus der obigen Meldung) AWS Systems Manager, zu Automatisierung wechseln und die Protokollausgabe auf die Ausführungs-ID überprüfen `eecdef79-9111-4532-921a-e098549f5259`.

Lösung eines bekannten Problems

- Problem: Die Bereitstellung der Lösung schlägt fehl und es wird ein Fehler angezeigt, der besagt, dass die Ressourcen bereits bei Amazon verfügbar sind CloudWatch.

Lösung: Suchen Sie im Abschnitt „CloudFormation Ressourcen/Ereignisse“ nach einer Fehlermeldung, die darauf hinweist, dass Protokollgruppen bereits vorhanden sind. Die SHARR Bereitstellungsvorlagen ermöglichen die Wiederverwendung vorhandener Protokollgruppen. Stellen Sie sicher, dass Sie die Wiederverwendung ausgewählt haben.

- Problem: Die Bereitstellung der Lösung schlägt fehl und es wird ein Fehler in einem verschachtelten Playbook-Stapel angezeigt, in dem eine EventBridge Regel nicht erstellt werden kann

Lösung: Sie haben wahrscheinlich das [Kontingent für EventBridge Regeln](#) mit der Anzahl der bereitgestellten Playbooks erreicht. Sie können dies vermeiden, indem Sie die [konsolidierten Kontrollergebnisse](#) in Security Hub zusammen mit dem SC-Playbook in dieser Lösung verwenden, nur die Playbooks für die verwendeten Standards bereitstellen oder eine Erhöhung des EventBridge Regelkontingents beantragen.

- Problem: Ich betreibe Security Hub in mehreren Regionen mit demselben Konto. Ich möchte diese Lösung in mehreren Regionen einsetzen.

Lösung: Stellen Sie den Admin-Stack im selben Konto und in derselben Region bereit wie Ihr Security Hub-Administrator. Installieren Sie die Mitgliedsvorlage in jedem Konto und jeder Region, in der Sie ein Security Hub Hub-Mitglied konfiguriert haben. Aktivieren Sie die Aggregation im Security Hub.

- Problem: Unmittelbar nach der Bereitstellung schlägt der SO0111- SHARR -Orchestrator im Status Get Automation Document mit einem 502-Fehler fehl: „Lambda konnte die Umgebungsvariablen nicht entschlüsseln, weil der Zugriff verweigert wurde. KMS Bitte überprüfen Sie die Tasteneinstellungen der Funktion. KMS Ausnahme: UnrecognizedClientException KMS Meldung: Das in der Anfrage enthaltene Sicherheitstoken ist ungültig. (Dienst: AWSLambda; Statuscode: 502; Fehlercode:KMSAccessDeniedException; Anforderungs-ID:...“

Lösung: Warten Sie etwa 10 Minuten, bis sich die Lösung stabilisiert hat, bevor Sie die Problembehebungen durchführen. Wenn das Problem weiterhin besteht, öffnen Sie ein Support-Ticket oder GitHub ein Problem.

- Problem: Ich habe versucht, ein Problem zu beheben, aber es ist nichts passiert.

Lösung: Suchen Sie in den Anmerkungen zu dem Ergebnis nach Gründen, warum das Problem nicht behoben wurde. Eine häufige Ursache ist, dass das Ergebnis nicht automatisch behoben werden kann. Derzeit gibt es keine Möglichkeit, dem Benutzer direktes Feedback zu geben, wenn keine Abhilfe gefunden wurde, außer über die Hinweise. Überprüfen Sie die Lösungsprotokolle. Öffnen Sie CloudWatch Logs in der Konsole. Suchen Sie die Gruppe SO0111- SHARR CloudWatch Logs. Sortieren Sie die Liste so, dass die zuletzt aktualisierten Streams zuerst angezeigt werden. Wählen Sie den Protokollstream für den Befund aus, den Sie auszuführen versucht haben. Sie sollten dort alle Fehler finden. Einige Gründe für den Fehler könnten sein: Diskrepanz zwischen der Kontrolle der Ergebnisse und der Behebungskontrolle, kontenübergreifende Problembehebung (noch nicht unterstützt) oder dass das Ergebnis bereits behoben wurde. Wenn Sie den Grund für den Fehler nicht ermitteln können, sammeln Sie bitte die Protokolle und öffnen Sie ein Support-Ticket.

- Problem: Nach dem Start einer Problembehebung wurde der Status in der Security Hub Hub-Konsole nicht aktualisiert.

Lösung: Die Security Hub Hub-Konsole wird nicht automatisch aktualisiert. Aktualisieren Sie die aktuelle Ansicht. Der Status des Ergebnisses sollte aktualisiert werden. Es kann mehrere Stunden dauern, bis das Ergebnis von „Fehlgeschlagen“ auf „Bestanden“ umgestellt wird. Ergebnisse werden anhand von Ereignisdaten erstellt, die von anderen Diensten wie AWS Config an AWS Security Hub gesendet werden. Die Zeit, bis eine Regel erneut bewertet wird, hängt vom zugrunde liegenden Dienst ab. Falls das Problem dadurch nicht behoben wird, finden Sie weitere Informationen unter „Ich habe versucht, ein Ergebnis zu korrigieren, aber es ist nichts passiert“.

- Problem: Die Orchestrator-Schrittfunktion schlägt im Status „Automationsdokument abrufen“ fehl: Beim Aufrufen des AssumeRole Vorgangs ist ein Fehler aufgetreten (AccessDenied).

Lösung: Die Mitgliedsvorlage wurde nicht in dem Mitgliedskonto installiert, in dem versucht SHARR wird, einen Fehler zu korrigieren. Folgen Sie den Anweisungen zur Bereitstellung der Mitgliedervorlage.

- Problem: Das Config.1-Runbook schlägt fehl, weil Recorder oder Delivery Channel bereits vorhanden sind.

Lösung: Überprüfen Sie Ihre AWS Config Einstellungen sorgfältig, um sicherzustellen, dass Config ordnungsgemäß eingerichtet ist. Die automatische Korrektur ist in einigen Fällen nicht in der Lage, bestehende AWS Konfigurationseinstellungen zu korrigieren.

- Problem: Die Behebung ist erfolgreich, es wird jedoch die Meldung zurückgegeben "No output available yet because the step is not successfully executed."

Lösung: Dies ist ein bekanntes Problem in dieser Version, bei dem bestimmte Reparatur-Runbooks keine Antwort zurückgeben. Die Reparatur-Runbooks schlagen ordnungsgemäß fehl und signalisieren die Lösung, wenn sie nicht funktionieren.

- Problem: Die Lösung ist fehlgeschlagen und es wurde ein Stack-Trace gesendet.

Lösung: Gelegentlich verpassen wir die Gelegenheit, eine Fehlerbedingung zu behandeln, die zu einem Stack-Trace und nicht zu einer Fehlermeldung führt. Versuchen Sie, das Problem anhand der Trace-Daten zu beheben. Öffnen Sie ein Support-Ticket, wenn Sie Hilfe benötigen.

- Problem: Das Entfernen des v1.3.0-Stacks ist auf der Ressource Custom Action fehlgeschlagen.

Lösung: Das Entfernen der Admin-Vorlage schlägt möglicherweise fehl, wenn die benutzerdefinierte Aktion entfernt wurde. Dies ist ein bekanntes Problem, das in der nächsten Version behoben wird. Wenn das passiert:

1. Melden Sie sich bei der [AWSSecurity Hub Hub-Verwaltungskonsolle](#) an.
2. Gehen Sie im Administratorkonto zu Einstellungen.
3. Wählen Sie den Tab Benutzerdefinierte Aktionen
4. Löschen Sie manuell den Eintrag Korrigieren mit SHARR.
5. Löschen Sie den Stapel erneut.

- Problem: Nach der erneuten Bereitstellung des Admin-Stacks schlägt die Step-Funktion fehl. AssumeRole

Lösung: Durch die erneute Bereitstellung des Admin-Stacks wird die Vertrauensverbindung zwischen der Administratorrolle im Administratorkonto und der Mitgliedsrolle in den Mitgliedskonten

unterbrochen. Sie müssen den Stack der Mitgliedsrollen in allen Mitgliedskonten erneut bereitstellen.

- Problem: CIS 3.x-Behebungen werden PASSED nach mehr als 24 Stunden nicht angezeigt.

Lösung: Dies kommt häufig vor, wenn Sie das S00111-SHARR_LocalAlarmNotification SNS Thema im Mitgliedskonto nicht abonniert haben.

Probleme mit bestimmten Abhilfemaßnahmen

S etSSLBucket Policy schlägt mit einem AccessDenied Fehler fehl

Zugeordnete Steuerelemente: AWS FSBP v1.0.0 S3.5, PCI v3.2.1 PCI S.3.5, v1.4.0 2.1.2, SC v2.0.0 S3.5 CIS

Problem: Die etSSLBucket S-Richtlinie schlägt mit AccessDenied einem Fehler fehl:

Beim Aufrufen des PutBucketPolicy Vorgangs ist ein Fehler aufgetreten (AccessDenied): Zugriff verweigert

Wenn die Einstellung „Öffentlichen Zugriff blockieren“ für einen Bucket aktiviert wurde, schlagen Versuche, eine Bucket-Richtlinie zu erstellen, die Anweisungen enthält, die öffentlichen Zugriff zulassen, mit diesem Fehler fehl. Dieser Status kann erreicht werden, indem eine Bucket-Richtlinie eingerichtet wird, die solche Anweisungen enthält, und dann die Sperrung des öffentlichen Zugriffs für diesen Bucket aktiviert wird.

Die Behebungskonfiguration S3 BucketPublicAccessBlock (zugehörige Steuerelemente: AWS FSBP v1.0.0 S3.2, PCI v3.2.1 PCI .S3.2, CIS v1.4.0 2.1.5.2, SC v2.0.0 S3.2) kann auch einen Bucket in diesen Status versetzen, da sie die Einstellung für den öffentlichen Zugriff festlegt, ohne die Bucket-Richtlinie zu ändern.

Die etSSLBucket S-Richtlinie fügt der Bucket-Richtlinie eine Anweisung hinzu, um Anfragen abzulehnen, die nicht verwendet werden. SSL Die anderen Anweisungen in der Richtlinie werden nicht geändert. Wenn es also Anweisungen gibt, die öffentlichen Zugriff zulassen, schlägt die Behebung fehl, wenn versucht wird, die geänderte Bucket-Richtlinie zu installieren, die diese Anweisungen immer noch enthält.

Lösung: Ändern Sie die Bucket-Richtlinie, um Aussagen zu entfernen, die öffentlichen Zugriff zulassen, die im Konflikt mit der Einstellung „öffentlichen Zugriff blockieren“ für den Bucket stehen.

PutS3 schlägt fehl BucketPolicyDeny

Dazugehörige Steuerungen: AWS FSBP v1.0.0 S3.6, NIST.800-53.r5 CA-9 (1), .800-53.r5 CM-2 NIST

Problem: Der BucketPolicyDeny PutS3 mit dem folgenden Fehler:

```
Unable to create an explicit deny statement for {bucket_name}.
```

Wenn die Prinzipale für alle Richtlinien im Ziel-Bucket „*“ lauten, kann die Lösung die Ablehnungsrichtlinie nicht zum Ziel-Bucket hinzufügen, da dadurch alle Bucket-Aktionen für alle Principals blockiert würden.

Lösung: Ändern Sie die Bucket-Richtlinie, um Aktionen für bestimmte Konten zuzulassen, anstatt „*“ -Prinzipale zu verwenden, und schränken Sie abgelehnte Aktionen ein.

Wie deaktiviere ich die Lösung

Im Falle eines Vorfalls stellen Sie möglicherweise fest, dass Sie die Lösung deaktivieren müssen, ohne die Infrastruktur zu entfernen. In diesen Szenarien wird detailliert beschrieben, wie verschiedene Komponenten in der Lösung deaktiviert werden.

Szenario 1: Deaktivieren Sie die automatische Korrektur für ein einzelnes Steuerelement.

1. Navigieren Sie EventBridge in der [AWS CloudFormation Konsole](#) zu.
2. Wählen Sie in der Seitenleiste Regeln aus.
3. Wählen Sie den Standard-Event-Bus aus und suchen Sie nach der Steuerung, die Sie deaktivieren möchten.
4. Wählen Sie die Regel aus und klicken Sie auf die Schaltfläche Deaktivieren.

Szenario 2: Deaktivieren Sie die automatische Korrektur für alle Kontrollen.

1. Navigieren Sie EventBridge in der Konsole zu.
2. Wählen Sie in der Seitenleiste Regeln aus.
3. Wählen Sie den „Standard“ -Event-Bus aus und wählen Sie unten alle Regeln aus.
4. Wählen Sie auf die Schaltfläche „Deaktivieren“. Beachten Sie, dass Sie dies möglicherweise für mehrere Seiten mit Regeln tun müssen.

Szenario 3: Deaktivieren Sie die manuelle Problembeseitigung für ein Konto

1. Navigieren Sie EventBridge in der Konsole zu.
2. Wählen Sie in der Seitenleiste Regeln aus.
3. Wählen Sie den „Standard“ -Event-Bus aus und suchen Sie nach „SHARRRemediate_with_“ CustomAction
4. Wählen Sie die Regel aus und klicken Sie auf die Schaltfläche „Deaktivieren“.

Kontakt Support

Wenn Sie [AWSDeveloper Support](#), [AWSBusiness Support](#) oder [AWSEnterprise Support](#) haben, können Sie das Support Center nutzen, um fachkundige Unterstützung zu dieser Lösung zu erhalten. In den folgenden Abschnitten finden Sie entsprechende Anweisungen.

Fall erstellen

1. Melden Sie sich im [Support Center](#) an.
2. Wählen Sie Create case (Fall erstellen) aus.

Wie können wir helfen?

1. Wählen Sie Technisch.
2. Wählen Sie für Service die Option Lösungen aus.
3. Wählen Sie als Kategorie die Option Andere Lösungen aus.
4. Wählen Sie unter Schweregrad die Option aus, die Ihrem Anwendungsfall am besten entspricht.
5. Wenn Sie den Service, die Kategorie und den Schweregrad eingeben, werden in der Benutzeroberfläche Links zu häufig gestellten Fragen zur Fehlerbehebung angezeigt. Wenn Sie Ihre Frage mit diesen Links nicht lösen können, wählen Sie Nächster Schritt: Zusätzliche Informationen.

Zusätzliche Informationen

1. Geben Sie als Betreff einen Text ein, der Ihre Frage oder Ihr Problem zusammenfasst.

2. Beschreiben Sie das Problem im Feld Beschreibung detailliert.
3. Wählen Sie Dateien anhängen.
4. Hängen Sie die Informationen an, die Support für die Bearbeitung der Anfrage erforderlich sind.

Helfen Sie uns, Ihren Fall schneller zu lösen

1. Geben Sie die angeforderten Informationen ein.
2. Klicken Sie auf Next step: Solve now or contact us (Nächster Schritt): Jetzt lösen oder Support kontaktieren).

Löse es jetzt oder kontaktiere uns

1. Sehen Sie sich die Solve Now-Lösungen an.
2. Wenn Sie Ihr Problem mit diesen Lösungen nicht lösen können, wählen Sie Kontaktieren Sie uns, geben Sie die angeforderten Informationen ein und klicken Sie auf Absenden.

Deinstalliere die Lösung

Gehen Sie wie folgt vor, um die Lösung mit dem zu deinstallieren AWS Management Console.

V1.0.0-V1.2.1

Verwenden Sie für die Versionen v1.0.0 bis v1.2.1 Service Catalog, um die CIS und/oder Playbooks zu deinstallieren. FSBP Mit v1.3.0 wird Service Catalog nicht mehr verwendet.

1. Melden Sie sich an der [AWS CloudFormation Konsole](#) an und navigieren Sie zum Security Hub Hub-Hauptkonto.
2. Wählen Sie Service Catalog, um alle bereitgestellten Playbooks zu beenden und alle Sicherheitsgruppen, Rollen oder Benutzer zu entfernen.
3. Entfernen Sie die `CISPermissions.template` Spoke-Vorlage aus den Security Hub Hub-Mitgliedskonten.
4. Entfernen Sie die `AFSBPMemberStack.template` Spoke-Vorlage aus den Security Hub-Administrator- und Mitgliedskonten.
5. Navigieren Sie zum Security Hub Hub-Hauptkonto, wählen Sie den Installationsstapel der Lösung aus und wählen Sie dann Löschen aus.

Note

CloudWatch Protokolle Gruppenprotokolle werden aufbewahrt. Wir empfehlen, diese Protokolle so aufzubewahren, wie es die Protokollaufbewahrungsrichtlinie Ihres Unternehmens vorschreibt.

V1.3.x

1. Entfernen Sie das `aws-sharr-member.template` von jedem Mitgliedskonto.
2. Entfernen Sie das `aws-sharr-admin.template` aus dem Administratorkonto.

Note

Das Entfernen der Admin-Vorlage in Version 1.3.0 schlägt wahrscheinlich fehl, wenn die benutzerdefinierte Aktion entfernt wird. Dies ist ein bekanntes Problem, das in der nächsten Version behoben wird. Verwenden Sie die folgenden Anweisungen, um dieses Problem zu beheben:

1. Melden Sie sich bei der [AWS Security Hub Hub-Verwaltungskonsole](#) an.
2. Gehen Sie im Administratorkonto zu Einstellungen.
3. Wählen Sie den Tab Benutzerdefinierte Aktionen aus.
4. Löschen Sie manuell den Eintrag Korrigieren mit SHARR.
5. Löschen Sie den Stapel erneut.

V1.4.0 und höher

Stack-Bereitstellung

1. Entfernen Sie das `aws-sharr-member.template` aus jedem Mitgliedskonto.
2. Entfernen Sie das `aws-sharr-admin.template` aus dem Administratorkonto.

StackSet Bereitstellung

Entfernen Sie für jeden StackSet Stapel und entfernen Sie dann die Stapel StackSet in umgekehrter Reihenfolge der Bereitstellung.

Beachten Sie, dass IAM Rollen aus dem beibehalten `aws-sharr-member-roles.template` werden, auch wenn die Vorlage entfernt wird. Auf diese Weise können Behebungen, die diese Rollen verwenden, weiterhin funktionieren. Diese SO0111-*-Rollen können manuell entfernt werden, nachdem sichergestellt wurde, dass sie nicht mehr verwendet werden, und zwar durch aktive Behebungsmaßnahmen, z. B. CloudTrail zur Protokollierung oder zur erweiterten Überwachung.

CloudWatch RDS

Administratorhandbuch

Teile der Lösung aktivieren und deaktivieren

Als Lösungsadministrator haben Sie die folgenden Möglichkeiten, festzulegen, welche Funktionen der Lösung aktiviert werden.

Wo die Stacks für Mitglieder und Mitgliederrollen bereitgestellt werden:

- Der Admin-Stack kann Abhilfemaßnahmen (durch benutzerdefinierte Aktionen oder vollautomatische EventBridge Regeln) nur für Konten einleiten, in denen die Mitglieder- und Mitgliederrollen-Stacks mit der als Parameterwert angegebenen Admin-Kontonummer bereitgestellt wurden.
- Um Konten oder Regionen vollständig von der Kontrolle über die Lösung auszunehmen, sollten Sie die Rollenstapel für Mitglieder oder Mitglieder nicht für diese Konten oder Regionen bereitstellen.

Suche nach der Aggregationskonfiguration für Konto und Region in Security Hub:

- Der Admin-Stack ist nur in der Lage, Problembehebungen (durch benutzerdefinierte Aktionen oder vollautomatische EventBridge Regeln) für Ergebnisse einzuleiten, die im Administratorkonto und in der Region eingehen.
- Um Konten oder Regionen vollständig von der Kontrolle über die Lösung auszunehmen, schließen Sie diese Konten oder Regionen nicht ein, um Ergebnisse an dasselbe Administratorkonto und dieselbe Region zu senden, in der der Admin-Stack bereitgestellt wird.

Welche verschachtelten Standard-Stacks werden bereitgestellt:

- Der Admin-Stack ist nur in der Lage, Korrekturen (durch benutzerdefinierte Aktionen oder vollautomatische EventBridge Regeln) für Kontrollen einzuleiten, für die ein Kontroll-Runbook im Zielmitgliedskonto und in der Zielregion bereitgestellt wurde. Diese werden vom Mitgliedsstapel für jeden Standard bereitgestellt.
- Der Admin-Stack kann nur vollautomatische Problembehebungen einleiten, indem er EventBridge Regeln für Kontrollen verwendet, für die die Regeln gelten, die vom Admin-Stack für diesen Standard bereitgestellt werden. Diese werden für das Administratorkonto bereitgestellt.
- Der Einfachheit halber empfehlen wir die einheitliche Implementierung von Standards für Ihre Administrator- und Mitgliedskonten. Wenn Sie sich für AWS FSBP und CIS v1.2.0 interessieren,

stellen Sie diese beiden verschachtelten Admin-Stacks für das Administratorkonto bereit und stellen Sie diese beiden verschachtelten Mitglieds-Stacks für jedes Mitgliedskonto und jede Region bereit.

Welche Control-Runbooks werden in jedem verschachtelten Mitgliedsstapel bereitgestellt:

- Der Admin-Stack ist nur in der Lage, Korrekturen (durch benutzerdefinierte Aktionen oder vollautomatische EventBridge Regeln) für Kontrollen einzuleiten, bei denen für jeden Standard ein Kontroll-Runbook im Zielmitgliedskonto und in der Region vom Mitgliedsstapel bereitgestellt wird.
- Um eine genauere Kontrolle darüber zu haben, welche Kontrollen für einen bestimmten Standard aktiviert werden, enthält jeder verschachtelte Stack für einen Standard Parameter, für die Kontroll-Runbooks bereitgestellt werden. Setzen Sie den Parameter für ein Steuerelement auf den Wert „NOTVerfügbar“, um die Bereitstellung dieses Kontroll-Runbooks aufzuheben.

SSMParameter für die Aktivierung und Deaktivierung von Standards:

- Der Admin-Stack kann nur Korrekturen (durch benutzerdefinierte Aktionen oder vollautomatische EventBridge Regeln) für Standards einleiten, die über den vom Standard-Admin-Stack bereitgestellten SSM Parameter aktiviert wurden.
- <standard_name><standard_version>Um einen Standard zu deaktivieren, setzen Sie den Wert für den SSM Parameter mit dem Pfad „/solutions/SO0111///status“ auf „Nein“.

Beispiele für Benachrichtigungen SNS

Wenn eine Problembhebung eingeleitet wird

```
{
  "severity": "INFO",
  "message": "00000000-0000-0000-0000-000000000000: Remediation queued for SC control RDS.13 in account 111111111111",
  "finding": {
    "finding_id": "22222222-2222-2222-2222-222222222222",
    "finding_description": "This control checks if automatic minor version upgrades are enabled for the Amazon RDS database instance.",
    "standard_name": "security-control",
    "standard_version": "2.0.0",
    "standard_control": "RDS.13",
```

```

    "title": "RDS automatic minor version upgrades should be enabled",
    "region": "us-east-1",
    "account": "111111111111",
    "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/finding/22222222-2222-2222-2222-222222222222"
  }
}

```

Wenn eine Sanierung erfolgreich ist

```

{
  "severity": "INFO",
  "message": "00000000-0000-0000-0000-000000000000: Remediation succeeded for SC control RDS.13 in account 111111111111: See Automation Execution output for details (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
  "finding": {
    "finding_id": "22222222-2222-2222-2222-222222222222",
    "finding_description": "This control checks if automatic minor version upgrades are enabled for the Amazon RDS database instance.",
    "standard_name": "security-control",
    "standard_version": "2.0.0",
    "standard_control": "RDS.13",
    "title": "RDS automatic minor version upgrades should be enabled",
    "region": "us-east-1",
    "account": "111111111111",
    "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/finding/22222222-2222-2222-2222-222222222222"
  }
}

```

Wenn eine Behebung fehlschlägt

```

{
  "severity": "ERROR",
  "message": "00000000-0000-0000-0000-000000000000: Remediation failed for SC control RDS.13 in account 111111111111: See Automation Execution output for details (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
  "finding": {

```

```
"finding_id": "22222222-2222-2222-2222-222222222222",
"finding_description": "This control checks if automatic minor version upgrades are
enabled for the Amazon RDS database instance.",
"standard_name": "security-control",
"standard_version": "2.0.0",
"standard_control": "RDS.13",
"title": "RDS automatic minor version upgrades should be enabled",
"region": "us-east-1",
"account": "111111111111",
"finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
}
}
```

Benutze die Lösung

Dies ist ein Tutorial, das Sie durch Ihre erste Bereitstellung von führtASR. Es beginnt mit den Voraussetzungen für die Bereitstellung der Lösung und endet damit, dass Sie Beispielprobleme in einem Mitgliedskonto korrigieren.

Tutorial: Erste Schritte mit Automated Security Response on AWS

Dies ist ein Tutorial, das Sie durch Ihre erste Implementierung führt. Es beginnt mit den Voraussetzungen für die Bereitstellung der Lösung und endet damit, dass Sie Beispielprobleme in einem Mitgliedskonto korrigieren.

Bereiten Sie die Konten vor

Um die kontenübergreifenden und regionsübergreifenden Problembhebungsmöglichkeiten der Lösung zu demonstrieren, werden in diesem Tutorial zwei Konten verwendet. Sie können die Lösung auch für ein einzelnes Konto bereitstellen.

In den folgenden Beispielen werden Konten verwendet 111111111111 und 222222222222 die Lösung demonstriert. 111111111111 wird das Administratorkonto und 222222222222 das Mitgliedskonto sein. Wir werden die Lösung zur Behebung von Problemen mit Ressourcen in den Regionen us-east-1 und us-west-2 einrichten.

Die folgende Tabelle ist ein Beispiel zur Veranschaulichung der Maßnahmen, die wir für jeden Schritt in jedem Konto und jeder Region ergreifen werden.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Keine	None
222222222222	Mitglied	Keine	None

Das Administratorkonto ist das Konto, das die Verwaltungsaktionen der Lösung ausführt, d. h. die manuelle Initiierung von Problembhebungen oder die Aktivierung einer vollautomatischen Problembhebung mit Regeln. EventBridge Dieses Konto muss auch das delegierte Security Hub-Administratorkonto für alle Konten sein, bei denen Sie Fehler korrigieren möchten. Es muss und sollte jedoch nicht das Administratorkonto der AWS AWS Organisation sein, zu der Ihre Konten gehören.

AWSConfig aktivieren

Lesen Sie die folgende Dokumentation:

- [AWSDokumentation zur Config](#)
- [AWSPreisgestaltung Config](#)
- [AWSConfig aktivieren](#)

Aktivieren Sie AWS Config in beiden Konten und beiden Regionen. Dies wird mit Gebühren verbunden sein.

Important

Stellen Sie sicher, dass Sie die Option „Globale Ressourcen (z. B. AWS IAM Ressourcen) einbeziehen“ auswählen. Wenn Sie diese Option bei der Aktivierung von AWS Config nicht auswählen, werden Ihnen keine Ergebnisse zu globalen Ressourcen (z. B. AWS IAM Ressourcen) angezeigt.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	AWSConfig aktivieren	AWSConfig aktivieren
222222222222	Mitglied	AWSConfig aktivieren	AWSConfig aktivieren

Aktivieren Sie den AWS Sicherheitshub

Lesen Sie die folgende Dokumentation:

- [AWS Security Hub Hub-Dokumentation](#)
- [AWS Security Hub Hub-Preise](#)
- [AWS Security Hub aktivieren](#)

Aktivieren Sie AWS Security Hub in beiden Konten und beiden Regionen. Dies wird mit Gebühren verbunden sein.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	AWS Security Hub aktivieren	AWS Security Hub aktivieren
222222222222	Mitglied	AWS Security Hub aktivieren	AWS Security Hub aktivieren

Ermöglichen Sie konsolidierte Kontrollergebnisse

Lesen Sie die folgende Dokumentation:

- [Generierung und Aktualisierung der Kontrollergebnisse](#)

In diesem Tutorial werden wir die Verwendung der Lösung bei aktivierter Funktion für konsolidierte Kontrollergebnisse von AWS Security Hub demonstrieren, was die empfohlene Konfiguration ist. In Partitionen, die diese Funktion zum Zeitpunkt der Erstellung dieses Artikels nicht unterstützen, müssen Sie statt SC (Security Control) die standardspezifischen Playbooks bereitstellen.

Ermöglichen Sie konsolidierte Kontrollergebnisse für beide Konten und beide Regionen.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Ermöglichen Sie konsolidierte Kontrolle rgebnisse	Ermöglichen Sie konsolidierte Kontrolle rgebnisse
222222222222	Mitglied	Ermöglichen Sie konsolidierte Kontrolle rgebnisse	Ermöglichen Sie konsolidierte Kontrolle rgebnisse

Es kann einige Zeit dauern, bis mit der neuen Funktion Ergebnisse generiert werden. Sie können mit dem Tutorial fortfahren, aber Sie können die ohne die neue Funktion generierten Ergebnisse nicht korrigieren. Mit der neuen Funktion generierte Ergebnisse können anhand des GeneratorId Feldwerts `security-control/<control_id>` identifiziert werden.

Konfigurieren Sie die regionsübergreifende Suchaggregation

Lesen Sie die folgende Dokumentation:

- [Regionsübergreifende Aggregation](#)
- [Aktivierung der regionsübergreifenden Aggregation](#)

Konfigurieren Sie die Suchaggregation von us-west-2 bis us-east-1 in beiden Konten.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Konfigurieren Sie die Aggregation von us-west-2	None
222222222222	Mitglied	Konfigurieren Sie die Aggregation von us-west-2	None

Es kann einige Zeit dauern, bis die Ergebnisse in die Aggregationsregion übertragen werden. Sie können mit dem Tutorial fortfahren, aber Sie können Ergebnisse aus anderen Regionen erst korrigieren, wenn sie in der Aggregationsregion angezeigt werden.

Benennen Sie ein Security Hub-Administratorkonto

Lesen Sie die folgende Dokumentation:

- [Konten in AWS Security Hub verwalten](#)
- [Konten von Mitgliedern der Organisation verwalten](#)
- [Verwaltung von Mitgliedskonten auf Einladung](#)

Im folgenden Beispiel verwenden wir die manuelle Einladungsmethode. Für eine Reihe von Produktionskonten empfehlen wir, die delegierte Security Hub-Administration über AWS Organizations zu verwalten.

Laden Sie über die AWS Security Hub-Konsole im Administratorkonto (111111111111) das Mitgliedskonto (222222222222) ein, das Administratorkonto als delegierten Security Hub-Administrator zu akzeptieren. Nehmen Sie die Einladung vom Mitgliedskonto aus an.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Laden Sie das Mitgliedskonto ein	None
222222222222	Mitglied	Nehmen Sie die Einladung an	None

Es kann einige Zeit dauern, bis die Ergebnisse auf das Administratorkonto übertragen werden. Sie können mit dem Tutorial fortfahren, aber Sie können Ergebnisse aus Mitgliedskonten erst korrigieren, wenn sie im Administratorkonto angezeigt werden.

Erstellen Sie die Rollen für selbstverwaltete Berechtigungen StackSets

Lesen Sie die folgende Dokumentation:

- [AWS CloudFormation StackSets](#)
- [Gewähren Sie selbstverwaltete Berechtigungen](#)

Wir werden CloudFormation Stacks für mehrere Konten bereitstellen, also verwenden wir StackSets. Wir können keine vom Dienst verwalteten Berechtigungen verwenden, da der Admin-Stack und der Member-Stack verschachtelte Stacks haben, die vom Dienst nicht unterstützt werden. Daher müssen wir selbstverwaltete Berechtigungen verwenden.

Stellen Sie die Stacks für grundlegende Berechtigungen für Operationen bereit. StackSet Für Produktionskonten empfiehlt es sich möglicherweise, die Berechtigungen entsprechend der Dokumentation zu den „erweiterten Berechtigungsoptionen“ einzuschränken.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Stellen Sie den StackSet Administr	None

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
		ator-Rollenstapel bereit	
		Stellen Sie den StackSet Ausführungs-Rollenstapel bereit	
222222222222	Mitglied	Stellen Sie den StackSet Ausführungsrollen-Stack bereit	None

Erstellen Sie die unsicheren Ressourcen, die zu Beispielergebnissen führen

Lesen Sie die folgende Dokumentation:

- [Referenz zu Security Hub-Steuerungen](#)
- [AWSLambda-Steuerungen](#)

Die folgende Beispielressource mit einer unsicheren Konfiguration soll eine Problembehebung demonstrieren. Die Beispielsteuerung ist Lambda.1: Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten.

Important

Wir werden absichtlich eine Ressource mit einer unsicheren Konfiguration erstellen. Bitte überprüfen Sie die Art der Kontrolle und bewerten Sie selbst das Risiko, das mit der Erstellung einer solchen Ressource in Ihrer Umgebung verbunden ist. Machen Sie sich bewusst, über welche Tools Ihr Unternehmen möglicherweise verfügt, um solche Ressourcen zu erkennen und zu melden, und beantragen Sie gegebenenfalls eine Ausnahme. Wenn das von uns ausgewählte Steuerelement für Sie nicht geeignet ist, wählen Sie ein anderes Steuerelement aus, das von der Lösung unterstützt wird.

Navigieren Sie in der zweiten Region des Mitgliedskontos zur AWS Lambda-Konsole und erstellen Sie eine Funktion in der neuesten Python-Laufzeit. Fügen Sie unter Konfiguration -> Berechtigungen

eine Richtlinienanweisung hinzu, um das Aufrufen der Funktion ohne Authentifizierung von aus zu ermöglichen. URL

Vergewissern Sie sich auf der Konsolenseite, dass die Funktion öffentlich zugänglich ist. Nachdem die Lösung dieses Problem behoben hat, vergleichen Sie die Berechtigungen, um sicherzustellen, dass der öffentliche Zugriff gesperrt wurde.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Keine	None
222222222222	Mitglied	None	Erstellen Sie eine Lambda-Funktion mit einer unsicheren Konfiguration

Es kann einige Zeit dauern, bis AWS Config die unsichere Konfiguration erkennt. Sie können mit dem Tutorial fortfahren, aber Sie können das Ergebnis erst korrigieren, wenn Config es erkennt.

Erstellen Sie CloudWatch Protokollgruppen für verwandte Steuerelemente

Lesen Sie die folgende Dokumentation:

- [Überwachen von CloudTrail Protokolldateien mit Amazon CloudWatch Logs](#)
- [CloudTrail Kontrollen](#)

Verschiedene CloudTrail Steuerelemente, die von der Lösung unterstützt werden, setzen voraus, dass es eine CloudWatch Protokollgruppe gibt, die das Ziel einer Multiregion CloudTrail ist. Im folgenden Beispiel werden wir eine Platzhalter-Protokollgruppe erstellen. Für Produktionskonten sollten Sie die CloudTrail Integration mit CloudWatch Logs ordnungsgemäß konfigurieren.

Erstellen Sie in jedem Konto und jeder Region eine Protokollgruppe mit demselben Namen, zum Beispiel: `asr-log-group`.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Eine Protokollgruppe erstellen	Eine Protokollgruppe erstellen
222222222222	Mitglied	Eine Protokollgruppe erstellen	Eine Protokollgruppe erstellen

Stellen Sie die Lösung für Tutorial-Konten bereit

Sammeln Sie die drei Amazon S3 S3-Rollen URLs für den Rollenstapel „Administrator“, „Mitglied“ und „Mitglied“.

Stellen Sie den Admin-Stack bereit

[View template](#)

aws-

[sharr-deploy.vorlage](#)

Navigieren Sie im Administratorkonto zur CloudFormation Konsole und stellen Sie den Admin-Stack in der Security Hub-Suchaggregationsregion bereit.

Wählen Sie No den Wert aller Parameter für das Laden verschachtelter Admin-Stacks mit Ausnahme des Stacks „SC“ oder „Security Control“ aus. Dieser Stack enthält die Ressourcen für die konsolidierten Kontrollergebnisse, die wir in unseren Konten konfiguriert haben.

Entscheiden Sie sich No für die Wiederverwendung der Orchestrator-Protokollgruppe, sofern Sie diese Lösung nicht schon einmal für dieses Konto und diese Region bereitgestellt haben.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Stellen Sie den Admin-Stack bereit	None
222222222222	Mitglied	Keine	None

Warten Sie, bis der Admin-Stack die Bereitstellung abgeschlossen hat, bevor Sie fortfahren, damit eine Vertrauensbeziehung zwischen den Mitgliedskonten und dem Administratorkonto hergestellt werden kann.

Stellen Sie den Mitglieds-Stack bereit

[View template](#)

aws-

[sharr-member](#).vorlage

Navigieren Sie im Administratorkonto zur CloudFormation StackSets Konsole und stellen Sie den Mitgliederstapel für jedes Konto und jede Region bereit. Verwenden Sie die in diesem Tutorial erstellten StackSets Admin- und Ausführungsrollen.

Geben Sie den Namen der Protokollgruppe, die Sie erstellt haben, als Wert für den Parameter für den Protokollgruppennamen ein.

Wählen Sie No den Wert aller Parameter für das Laden verschachtelter Mitgliedsstapel mit Ausnahme des Stacks „SC“ oder „Security Control“ aus. Dieser Stapel enthält die Ressourcen für die konsolidierten Kontrollergebnisse, die wir in unseren Konten konfiguriert haben.

Geben Sie die ID des Administratorkontos als Wert für den Parameter für die Admin-Kontonummer ein. In unserem Beispiel ist das 111111111111.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Das Mitglied bereitstellen StackSet //Bestätigen Sie die Bereitstellung des Mitglieds-Stacks	Bestätigen Sie den bereitgestellten Mitglieds-Stack
222222222222	Mitglied	Bestätigen Sie den bereitgestellten Mitglieds-Stack	Bestätigen Sie den bereitgestellten Mitglieds-Stack

Stellen Sie den Mitgliederrollen-Stack bereit

[View template](#)

aws-

[sharr-member-roles](#).vorlage

Navigieren Sie im Administratorkonto zur CloudFormation StackSets Konsole und stellen Sie den Mitglieds-Stack für jedes Konto bereit. Verwenden Sie die in diesem Tutorial erstellten StackSets Admin- und Ausführungsrollen. Geben Sie die ID des Administratorkontos als Wert für den Parameter für die Admin-Kontonummer ein. In unserem Beispiel ist das 111111111111.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Das Mitglied bereitstellen StackSet //Bestätigen Sie die Bereitstellung des Mitglieds-Stacks	None
222222222222	Mitglied	Bestätigen Sie den bereitgestellten Mitglieds-Stack	None

Sie können fortfahren, aber Sie können die Ergebnisse erst korrigieren, wenn die Bereitstellung CloudFormation StackSets abgeschlossen ist.

Abonnieren Sie das Thema SNS

Aktualisierungen zur Problembeseitigung

Thema — [SO0111](#) — _Thema SHARR

Abonnieren Sie im Admin-Konto das SNS Amazon-Thema, das vom Admin-Stack erstellt wurde. Dadurch werden Sie benachrichtigt, wenn Abhilfemaßnahmen eingeleitet werden und wann sie erfolgreich sind oder fehlschlagen.

Alarmer

Thema - [SO0111](#) - _Alarm_Topic ASR

Abonnieren Sie im Admin-Konto das SNS Amazon-Thema, das vom Admin-Stack erstellt wurde. Dadurch werden Sie benachrichtigt, wenn metrische Alarme ausgelöst werden.

Korrigieren Sie die Ergebnisse der Beispiele

Navigieren Sie im Administratorkonto zur Security Hub Hub-Konsole und suchen Sie nach dem Ergebnis für die Ressource mit unsicherer Konfiguration, die Sie im Rahmen dieses Tutorials erstellt haben.

Dies kann auf verschiedene Arten geschehen:

1. In Partitionen, die die Funktion für konsolidierte Kontrollergebnisse unterstützen, können Sie auf einer Seite mit der Bezeichnung „Kontrollen“ die Ergebnisse anhand der konsolidierten Kontroll-ID suchen.
2. Auf der Seite „Sicherheitsstandards“ können Sie das Steuerelement danach suchen, zu welchem Standard es gehört.
3. Sie können alle Ergebnisse auf der Seite „Ergebnisse“ einsehen und nach Attributen suchen.

Die konsolidierte Kontroll-ID für die öffentliche Lambda-Funktion, die wir erstellt haben, ist Lambda.1.

Initiieren Sie die Behebung

Aktivieren Sie das Kontrollkästchen links neben dem Ergebnis, das sich auf die von uns erstellte Ressource bezieht. Wählen Sie im Drop-down-Menü „Aktionen“ die Option „Korrigieren mitASR“ aus. Sie erhalten eine Benachrichtigung, dass das Ergebnis an Amazon gesendet wurde EventBridge.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Initiieren Sie die Sanierung	None
222222222222	Mitglied	Keine	None

Vergewissern Sie sich, dass das Problem durch die Behebung behoben wurde

Sie sollten zwei SNS Benachrichtigungen erhalten. Die erste gibt an, dass eine Wiederherstellung eingeleitet wurde, und die zweite gibt an, dass die Wiederherstellung erfolgreich war. Navigieren Sie nach Erhalt der zweiten Benachrichtigung zur Lambda-Konsole im Mitgliedskonto und bestätigen Sie, dass der öffentliche Zugriff gesperrt wurde.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Keine	None
222222222222	Mitglied	None	Vergewissern Sie sich, dass die Behebung erfolgreich war

Verfolgen Sie die Ausführung der Behebung

Um besser zu verstehen, wie die Lösung funktioniert, können Sie die Ausführung der Behebung nachverfolgen.

EventBridge Regel

Suchen Sie im Administratorkonto nach einer EventBridge Regel mit dem Namen SHARRRemediate_with_.. CustomAction Diese Regel entspricht dem Ergebnis, das Sie von Security Hub gesendet haben, und sendet ihn an die Orchestrator Step Functions.

Ausführung von Step Functions

Suchen Sie im Administratorkonto nach den AWS Step Functions mit dem Namen "SO0111- SHARR -Orchestrator". Diese Schrittfunktion ruft das SSM Automatisierungsdokument im Zielkonto und in der Region auf. Sie können die Ausführung der Behebung in der Ausführungshistorie dieser AWS Step Functions verfolgen.

SSM-Automatisierung

Navigieren Sie im Mitgliedskonto zur SSM Automation-Konsole. Sie finden zwei Ausführungen eines Dokuments mit dem Namen "ASR-SC_2.0.0_Lambda.1" und eine Ausführung eines Dokuments mit dem Namen "-". ASR RemoveLambdaPublicAccess

Die erste Ausführung erfolgt über die Orchestrator-Step-Funktion im Zielkonto. Die zweite Ausführung erfolgt in der Zielregion, die möglicherweise nicht die Region ist, aus der das Ergebnis stammt. Die endgültige Ausführung ist die Behebung, bei der die Richtlinie für den öffentlichen Zugriff aus der Lambda-Funktion aufgehoben wird.

CloudWatch Gruppe protokollieren

Navigieren Sie im Administratorkonto zur CloudWatch Logs-Konsole und suchen Sie nach einer Protokollgruppe mit dem Namen "SO0111- SHARR". Diese Protokollgruppe ist das Ziel für High-Level-Logs aus den Orchestrator Step Functions.

Ermöglichen Sie vollautomatische Problembehebungen

Die andere Betriebsart der Lösung besteht darin, Ergebnisse automatisch zu korrigieren, sobald sie im Security Hub eingehen.

Vergewissern Sie sich, dass Sie über keine Ressourcen verfügen, auf die diese Feststellung möglicherweise versehentlich angewendet wird

Wenn Sie automatische Korrekturen aktivieren, werden Korrekturen für alle Ressourcen eingeleitet, die der von Ihnen aktivierten Steuerung entsprechen (Lambda.1).

Important

Bestätigen Sie, dass diese Berechtigung allen öffentlichen Lambda-Funktionen im Rahmen der Lösung entzogen werden soll. Vollautomatische Problembehebungen sind nicht auf die von Ihnen erstellte Funktion beschränkt. Die Lösung behebt diese Steuerung, wenn sie in einem der Konten und Regionen, in denen sie installiert ist, erkannt wird.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Bestätigen Sie, dass keine öffentlichen Funktionen gewünscht sind	Bestätigen Sie, dass keine öffentlichen Funktionen gewünscht sind
222222222222	Mitglied	Bestätigen Sie, dass keine öffentlichen Funktionen gewünscht sind	Bestätigen Sie, dass keine öffentlichen Funktionen gewünscht sind

Aktivieren Sie die Regel

Suchen Sie im Administratorkonto nach einer EventBridge Regel mit dem Namen `AutoTriggerSC_2.0.0_Lambda.1_` und aktivieren Sie sie.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Aktivieren Sie die automatisierten Behebungsregeln	None
222222222222	Mitglied	Keine	None

Konfigurieren Sie die Ressource

Konfigurieren Sie im Mitgliedskonto die Lambda-Funktion neu, um den öffentlichen Zugriff zu ermöglichen.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Keine	None
222222222222	Mitglied	None	Konfigurieren Sie die Lambda-Funktion, um

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
			öffentlichen Zugriff zu ermöglichen

Vergewissern Sie sich, dass das Problem durch die Behebung behoben wurde

Es kann einige Zeit dauern, bis Config die unsichere Konfiguration erneut erkennt. Sie sollten zwei SNS Benachrichtigungen erhalten. Die erste gibt an, dass eine Problembehebung eingeleitet wurde. Die zweite gibt an, dass die Behebung erfolgreich war. Navigieren Sie nach Erhalt der zweiten Benachrichtigung zur Lambda-Konsole im Mitgliedskonto und bestätigen Sie, dass der öffentliche Zugriff gesperrt wurde.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Aktivieren Sie die automatisierten Behebungsregeln	None
222222222222	Mitglied	None	Vergewissern Sie sich, dass die Behebung erfolgreich war

Bereinigen

Löschen Sie die Beispielressourcen

Löschen Sie im Mitgliedskonto die Lambda-Beispielfunktion, die Sie erstellt haben.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Keine	None

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
222222222222	Mitglied	None	Löschen Sie die Lambda-Beispielfunktion

Löschen Sie den Admin-Stack

Löschen Sie im Admin-Konto den Admin-Stack.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Löschen Sie den Admin-Stack	None
222222222222	Mitglied	Keine	None

Löschen Sie den Mitglieds-Stack

Löschen Sie das Mitglied im Admin-Konto StackSet.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Lösche das Mitglied StackSet Bestätigen Sie, dass die Mitgliederliste gelöscht	Bestätigen Sie, dass der Mitgliederstapel
222222222222	Mitglied	Bestätigen Sie, dass der Mitgliederstapel	Bestätigen Sie, dass der Mitgliederstapel

Löschen Sie den Stapel der Mitgliedsrollen

Löschen Sie im Admin-Konto die Mitgliedsrollen StackSet.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Löschen Sie die Mitgliederrollen StackSet Bestätigen Sie, dass der Rollenstapel gelöscht wurde	None
222222222222	Mitglied	Bestätigen Sie, dass der Rollenstapel für Mitglieder	None

Löschen Sie die beibehaltenen Rollen

Löschen Sie in jedem Konto die beibehaltenen IAM Rollen.

Wichtig: Diese Rollen werden für Behebungen beibehalten, für die eine Rolle erforderlich ist, damit die Korrektur weiterhin funktioniert (z. B. VPC Flow-Logging). Vergewissern Sie sich, dass Sie keine dieser Rollen weiterhin benötigen, bevor Sie sie löschen.

Löschen Sie alle Rollen mit dem Präfix SO0111 -.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Beibehaltene Rollen löschen	None
222222222222	Mitglied	Beibehaltene Rollen löschen	None

Planen Sie, dass die gespeicherten KMS Schlüssel gelöscht werden

Sowohl der Administrator- als auch der Mitgliederstapel erstellen und speichern einen KMS Schlüssel. Es fallen Gebühren an, wenn Sie diese Schlüssel behalten.

Diese Schlüssel werden aufbewahrt, damit Sie auf alle mit der Lösung verschlüsselten Ressourcen zugreifen können. Vergewissern Sie sich, dass Sie sie nicht benötigen, bevor Sie sie löschen möchten.

Identifizieren Sie die von der Lösung bereitgestellten Schlüssel anhand der von der Lösung erstellten Aliase oder anhand des CloudFormation Verlaufs. Planen Sie deren Löschung ein.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Identifizieren Sie den Administratorschlüssel und planen Sie ihn für die Löschung Identifizieren Sie den Mitgliedsschlüssel und planen Sie ihn für die Löschung	Identifizieren Sie den Mitgliedsschlüssel und planen Sie dessen Löschung
222222222222	Mitglied	Identifizieren Sie den Mitgliedsschlüssel und planen Sie dessen Löschung	Identifizieren Sie den Mitgliedsschlüssel und planen Sie dessen Löschung

Löschen Sie die Stacks für selbstverwaltete Berechtigungen StackSets

Löschen Sie die Stacks, die erstellt wurden, um selbstverwaltete Berechtigungen zu ermöglichen StackSets

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Löschen Sie den StackSet Administrator-Rollenstapel	None

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
222222222222	Mitglied	Löschen Sie den StackSet Ausführungsrollenstapel	None

Entwicklerhandbuch

Dieser Abschnitt enthält den Quellcode für die Lösung und zusätzliche Anpassungen.

Quellcode

Besuchen Sie unser [GitHub Repository](#), um die Vorlagen und Skripte für diese Lösung herunterzuladen und Ihre Anpassungen mit anderen zu teilen.

Spielbücher

[Diese Lösung umfasst die im Center for Internet Security \(CIS\) Foundations Benchmark v1.2.0, Foundations Benchmark v1.4.0, Foundations Benchmark v3.0.0, AWS Foundations Benchmarkv3.0.0, CIS AWS CIS AWS AWS FoundationalSecurity Best Practices \(FSBP\) v.1.0.0, Payment Card Industry Data Security Standard \(-\)v3.2.1 und National Institute of Standards definierten Sicherheitsstandards PCI DSS und Technologie \(\). NIST](#)

Wenn Sie konsolidierte Kontrollergebnisse aktiviert haben, werden diese Kontrollen in allen Standards unterstützt. Wenn diese Funktion aktiviert ist, muss nur das SC-Playbook bereitgestellt werden. Wenn nicht, werden die Playbooks für die zuvor aufgeführten Standards unterstützt.

Important

Stellen Sie die Playbooks nur für die aktivierten Standards bereit, um zu vermeiden, dass Servicekontingente erreicht werden.

Einzelheiten zu einer bestimmten Problembhebung finden Sie im Systems Manager Manager-Automatisierungsdokument mit dem Namen, der von der Lösung in Ihrem Konto bereitgestellt wird. Gehen Sie zur [AWSSystems Manager Manager-Konsole](#) und wählen Sie dann im Navigationsbereich Dokumente aus.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
Vollständige Abhilfemaßnahmen	63	34	29	33	65	19	90
ASR-EnableAutoScalingGroupELBHealthCheck Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten Load Balancer-Zustandspürungen verwenden	Autoscaling.1		Automatische Skalierung.1		Automatische Skalierung.1		Automatische Skalierung.1
ASR-Creat	CloudTrail.1.	2.1	CloudTrail.2.	3.1	CloudTrail.1.	3.1	CloudTrail.1.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
<p>eMultiRegionTrail</p> <p>CloudTrail sollte aktiviert und mit mindestens einem Multi-Region-Trail konfiguriert sein</p>							
<p>ASR-EnableEncryption</p> <p>CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben</p>	CloudTrail I2.	2.7	CloudTrail I1.	3.7	CloudTrail I2.	3.5	CloudTrail I2.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-EnableLogFileValidation Stellen Sie sicher, dass die Überprüfung der Protokolldatei aktiviert ist	CloudTrail 14.	2.2	CloudTrail 13.	3.2	CloudTrail 14.		CloudTrail 14.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-EnableCloudTrailToCloudWatchLogging Stellen Sie sicher, dass CloudTrail Trails in Amazon CloudWatch Logs integriert sind	CloudTrail 15.	2.4	CloudTrail 14.	3.4	CloudTrail 15.		CloudTrail 15.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-Konfiguriert 3 BucketLogging Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem S3-Bucket aktiviert ist CloudTrail		2.6		3.6		3.4	CloudTrail 17.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-ReplaceCodeBuildClearTextCredentials CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten	CodeBuild 2.		CodeBuild 2.		CodeBuild 2.		CodeBuild 2.
ASR-EnableAWSConfig Stelle sicher, dass AWS Config es aktiviert ist	Config.1	2.5	Config.1	3.5	Config.1	3.3	Config.1

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-M Private EBSSnapshots EBSAmazon - Snapshots sollten nicht öffentlich wiederherstellbar sein	EC21.		EC21.		EC21.		EC21.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-RemoveVPCdefaultSecurityGroupRulesVPCDie Standardsicherheit sgruppe sollte eingehenden und ausgehenden Datenverkehr verbieten	EC22.	4.3	EC22.	5.3	EC22.	5.4	EC22.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-E-Protokolle enableVPCFlow VPCDie Flow-Protokollierung sollte in allen aktiviert sein VPCs	EC26.	2,9	EC2.6	3.9	EC2.6	3.7	EC2.6
ASR-EnableEbsEncryptionByDefault EBSDie Standardverschlüsselung sollte aktiviert sein	EC27.	2.2.1			EC2.7	2.2.1	EC2.7

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
<p>ASR-RevokateUnrotatedKeys</p> <p>Die Zugangsschlüssel der Benutzer sollten alle 90 Tage oder weniger gewechselt werden</p>	IAM3.	1.4		1.14	IAM3.	1.14	IAM3.
<p>ASR-S-Richtlinie etIAMPassword</p> <p>IAMStandard-Passwortrichtlinie</p>	IAM7.	1,5-1,11	IAM.8	1.8	IAM.7	1.8	IAM.7

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR- Revoke UnusedIAM UserCred entials Benutzeran meldedat en sollten deaktivi ert werden, wenn sie nicht innerhalb von 90 Tagen verwendet werden	IAM8.	1.3	IAM.7		IAM.8		IAM.8

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR- RevokeUnusedIAMUserCredentials Benutzernmeldedaten sollten deaktiviert werden, wenn sie nicht innerhalb von 45 Tagen verwendet werden				1.12		1.12	IAM2.2

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-RemoveLambdaPublicAccessLambda-Funktionen sollten den öffentlichen Zugriff verbieten	Lambda.1		Lambda.1		Lambda.1		Lambda.1
ASR-MakeRDSSnapshotRDSSchnapschüsse sollten den öffentlichen Zugriff verbieten	RDS1.		RDS1.		RDS1.		RDS1.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-DisablePublicAccessToRDSInstance RDSDB-Instances sollten den öffentlichen Zugriff verbieten	RDS2.		RDS2.		RDS2.	2.3.3	RDS2.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-EncryptRDS Snapshot RDSCluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden	RDS4.				RDS4.		RDS4.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-EnableMultiAZonRDSInstance RDSDB-Instances sollten mit mehreren Availability Zones konfiguriert werden	RDS5.				RDS5.		RDS5.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-EnableEnhancedMonitoringOnRDSInstances Für RDS DB-Instances und Cluster sollte eine erweiterte Überwachung konfiguriert werden	RDS6.				RDS.6		RDS.6

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-EnableRDSCluster DeletionProtection RDSBei Clustern sollte der Lösenschutz aktiviert sein	RDS7.				RDS.7		RDS.7
ASR-EnableRDSInstance DeletionProtection RDSFür DB-Instances sollte der Lösenschutz aktiviert sein	RDS8.				RDS.8		RDS.8

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR- EnableMinorVersionUpgradeOnRDSEInstance RDSautomatische Upgrades kleinerer Versionen sollten aktiviert sein	RDS1.3				RDS.13	2.3.2	RDS.13
ASR- EnableCopyTagsToSnapshotOnRDSCluster RDSDB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren	RDS1.6				RDS.16		RDS.16

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-DisablePublicAccessToRedshiftCluster Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten	Redshift.1		Redshift.1		Redshift.1		Redshift.1

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-EnableAutomaticSnapshotsOnRedshiftCluster Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein	Redshift.3				Redshift.3		Redshift.3

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-EnableRedshiftClusterAuditLogging Amazon Redshift Redshift-Cluster sollte die Audit-Protokollierung aktiviert sein	Redshift.4				Redshift.4		Redshift.4

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR- Enabl eAutomati cVersionU pgradeOnR edshiftCl uster Bei Amazon Redshift sollten automatis che Upgrades auf Hauptvers ionen aktiviert sein	Redshift. 6				Redshift. 6		Redshift. 6

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-Konfiguriert 3 PublicAccessBlock Die Einstellung S3 Block Public Access sollte aktiviert sein	S3.1	2.3	S3.6	2.1.5.1	S3.1	2.1.4	S3.1
ASR-Konfiguriert 3 BucketPublicAccessBlock S3-Buckets sollten öffentlichen Lesezugriff verbieten	S3.2		S3.2	2.1.5.2	S3.2		S3.2

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-Konfiguriert 3 BucketPublicAccessBlock S3-Buckets sollten öffentlichen Schreibzugriff verbieten		S3.3					S3.3
ASR- S3 EnableDefaultEncryption Bei S3-Buckets sollte die serverseitige Verschlüsselung aktiviert sein	S3.4		S3.4	2.1.1	S3.4		S3.4

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-S Richtlinie etSSLBucket Für die Verwendung von S3-Buckets sollten Anfragen erforderlich sein SSL	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-S3 BlockDenylist Amazon S3 S3-Berechtigungen, die anderen AWS-Konten In-Bucket-Richtlinien gewährt wurden, sollten eingeschränkt werden	S3.6				S3.6		S3.6

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
Die Einstellung S3 Block Public Access sollte auf Bucket-Ebene aktiviert sein	S3.8				S3.8		S3.8

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-Konfiguriert 3 BucketPublicAccessBlock Stellen Sie sicher, dass der S3-Bucket, auf den sich die CloudTrail Anmeldung bezieht, nicht öffentlich zugänglich		2.3					CloudTrail6.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-CreateAccessLoggingBucket Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist		2.6					CloudTrail7.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-EnableKeyRotation Stellen Sie sicher, dass die Rotation für vom Kunden erstellte Dateien aktiviert CMKs ist		2.8	KMS1.	3.8	KMS4.	3.6	KMS4.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
<p>ASR-CreateLogMetricFilterAndAlarm</p> <p>Stellen Sie sicher, dass ein Log-Metricfilter und ein Alarm für unautorisierte API Anrufe vorhanden sind</p>		3.1		4.1			Cloudwatch.1

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Stellen Sie sicher, dass ein Log-Metricfilter und ein Alarm für AWS Management Console die Anmeldung ohne MFA		3.2		4.2			Cloudwatch.2

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
<p>ASR-CreateLogMetricFilterAndAlarm</p> <p>Stellen Sie sicher, dass ein Log-Metricfilter und ein Alarm für die Verwendung des Root-Benutzers vorhanden sind</p>		3.3	CW.1	4.3			Cloudwatch.3

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Stellen Sie sicher, dass ein Log-Metricfilter und ein Alarm für IAM Richtlinienänderungen vorhanden sind		3.4		4.4			Cloudwatch.4

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
<p>ASR-CreateLogMetricFilterAndAlarm</p> <p>Stellen Sie sicher, dass ein Log-Metricfilter und ein Alarm für Konfigurationsänderungen vorhanden sind</p> <p>CloudTrail</p>		3.5		4.5			Cloudwatch.5

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Stellen Sie sicher, dass ein Log-Metricfilter und ein Alarm für Authentifizierungsfehler vorhanden sind AWS Management Console		3.6		4.6			Cloudwatch.6

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
<p>ASR-CreateLogMetricFilterAndAlarm</p> <p>Stellen Sie sicher, dass ein Log-Metricfilter und ein Alarm vorhanden sind, um vom Kunden erstellte Dateien zu deaktivieren oder zu löschen CMKs</p>		3.7		4.7			Cloudwatch.7

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind		3.8		4.8			Cloudwatch.8

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Stellen Sie sicher, dass ein Log-Metricfilter und ein Alarm für Konfigurationsänderungen vorhanden sind AWS Config		3.9		4,9 bis 4,9			Cloudwatch.9

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Sicherheitsgruppe vorhanden sind		3.10		4,10			Cloudwatch.10

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
<p>ASR-CreateLogMetricFilterAndAlarm</p> <p>Stellen Sie sicher, dass ein Log-Metricfilter und ein Alarm für Änderungen an den Network Access Control Lists () vorhanden sind</p> <p>NACL</p>		3.11		4,11			Cloudwatch.11

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an NetworkGateways vorhanden sind		3.12		4,12			Cloudwatch.12

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-Creat eLogMetri cFilterAn dAlarm Sicherste llen, dass ein Protokoll metrikfil ter und ein Alarm für Änderunge n an der Routing- Tabelle vorhanden sind		3.13		4.13			Cloudwatc h.13

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Stellen Sie sicher, dass ein Log-Metricfilter und ein Alarm für Änderungen vorhanden sind VPC		3.14		4,14			Cloudwatch.14

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
<p>AWS-DisablePublicAccessForSecurityGroup</p> <p>Stellen Sie sicher, dass keine Sicherheitsgruppen den Zugang von 0.0.0.0/0 zu Port 22 zulassen</p>		4.1	EC25.		EC21.3		EC2.13

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
<p>AWS-DisablePublicAccessForSecurityGroup</p> <p>Stellen Sie sicher, dass keine Sicherheitsgruppen den Zugriff von 0.0.0.0/0 auf Port 3389 zulassen</p>		4.2			EC2.14		EC2.14
ASR-ConfigureNSTopicForStack	CloudFormation1.				CloudFormation1.		CloudFormation1.
ASR-CREATEIAMSupport		1.20		1,17		1,17	IAM1,8

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-DisablePublicIPAutoAssign EC2Amazon-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen	EC21.5				EC2.15		EC2.15
ASR-EnableCloudTrailLogFileValidation	CloudTrail4.	2.2	CloudTrail3.	3.2			CloudTrail4.
ASR-EnableEncryptionForSNSTopic	SNS1.				SNS1.		SNS1.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-EnableDeliveryStatusLoggingForSNSTopic Die Protokollierung des Zustellungsstatus sollte für Benachrichtigungen, die an ein Thema gesendet werden, aktiviert sein	SNS2.				SNS2.		SNS2.
ASR-EnableEncryptionForSQSQueue	SQS1.				SQS1.		SQS1.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-M PrivateRDS Snapshot Der Snapshot sollte privat sein	RDS1.		RDS1.				RDS1.
ASR-B SSMDokument PublicAccess SSMDokumente sollten nicht öffentlich sein	SSM4.				SSM4.		SSM4.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR- Enab eCloudFro ntDefault RootObjec t CloudFron t Bei Distribut ionen sollte ein Standard- Root- Objekt konfiguri ert sein	CloudFron t1.				CloudFron t1.		CloudFron t1.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-SetCloudFrontOriginDomainCloudFront Distributionen sollten nicht auf nicht existierende S3-Ursprünge verweisen	CloudFront 1.2				CloudFront 1.2		CloudFront 1.2

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-RemoveCodeBuildPrivilegedMode CodeBuild Projektumgebungen sollten eine AWS Config Protokollierungsdauer haben	CodeBuild 5.				CodeBuild 5.		CodeBuild 5.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-Terminieren EC2Instanzen Gestoppte EC2 Instanzen sollten nach einem bestimmten Zeitraum entfernt werden	EC24.				EC24.		EC24.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-Aktivieren IMDSV2On nstance EC2Instan zen sollten Instance Metadata Service Version 2 () IMDSv2 verwenden	EC2.8				EC2.8	5.6	EC2.8

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-Revok eUnauthor izedInbou dRules Sicherheitsgruppen sollten nur uneingesc hränkten eingehend en Verkehr für autorisie te Ports zulassen	EC21.8				EC2.18		EC2.18

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR- t DisableUn res rictedAcc essTo HighRiskP orts Sicherhei tsgruppen sollten keinen uneingesc hränkten Zugriff auf Ports mit hohem Risiko zulassen	EC21.9				EC2.19		EC2.19

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-DisableTGW AutoAcceptSharedAttachments AmazonEC2TransitGateways sollteVPC Anhangsanfragen nicht automatisch akzeptieren	EC22.3				EC22,3		EC22,3

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-EnablePrivateRepositoryScanning ECRBei privaten Repositorien sollte das Scannen von Bildern konfiguriert sein	ECR1.				ECR1.		ECR1.
ASR-EnableGuardDuty GuardDuty sollte aktiviert sein	GuardDuty1.		GuardDuty1.		GuardDuty1.		GuardDuty1.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-Konfiguriert 3 BucketLogging Die Protokollierung des S3-Bucket-Servers sollte aktiviert sein	S3.9				S3.9		S3.9
ASR-EnableBucketEventNotifications Bei S3-Buckets sollten Ereignisbenachrichtigungen aktiviert sein	S3.11				S3.11		S3.11

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
<p>ASR-Sets 3 Lifecycle Policy</p> <p>Für S3-Buckets sollten Lebenszyklusrichtlinien konfiguriert sein</p>	S3.13				S3.13		S3.13
<p>ASR-EnableAutoSecretRotation</p> <p>Secrets Manager Manager-Gheimnissen sollte die automatische Rotation aktiviert sein</p>	SecretsManager1.				SecretsManager1.		SecretsManager1.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-RemoveUnusedSecret Unbenutzte Secrets Manager Manager-Gheimnisse entfernen	SecretsManager3.				SecretsManager3.		SecretsManager3.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-UpdateSecretRotationPeriod Secrets Manager Manager-Gheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden	SecretsManager4.				SecretsManager4.		SecretsManager4.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-EnableAPIGatewayCacheDataEncryption					APIGateway5.		APIGateway5.
APIRESTAPIGateway-Cache-Daten sollten im Ruhezustand verschlüsselt werden							

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-SetLogGroupRetentionDays CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden					CloudWatch 1.6		CloudWatch.16

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR- Attac hServiceV PCEndpoin t Amazon EC2 sollte so konfiguri ert sein, dass es VPC Endpunkte verwendet , die für den EC2 Amazon- Service erstellt wurden	EC21.0				EC2.10		EC2.10
ASR- TagGu ardDutyRe source GuardDuty Filter sollten markiert werden							GuardDuty 2.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-TagGuardDutyResource GuardDuty Detektoren sollten markiert werden							GuardDuty 4.
ASRttachSSMPermissions-Zu EC2 EC2Amazon-Instances sollten von Systems Manager verwaltet werden	SSM1.		SSM3.				SSM1.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-ConfigureLaunchConfigurationPublicIPDocument					AutoScaling.5		AutoScaling.5
EC2Amazon-Instances, die mit Auto Scaling Gruppen gestartet wurden, sollten keine öffentlichen IP-Adressen haben							
ASR-EnableAPIGatewayExecutionLogs	APIGateway1.						APIGateway1.

Beschreibung	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISVersion 1.4.0	NIST	CISv3.0.0	ID der Sicherheitskontrolle
ASR-EnableMacie Amazon Macie sollte aktiviert sein	Macie.1				Macie.1		Macie.1
ASR-EnableAthenaWorkGroupLogging Athena Arbeitsgruppen sollte die Protokollierung aktiviert sein	Athena.4						Athena.4

Hinzufügen neuer Abhilfemaßnahmen

Das Hinzufügen einer neuen Abhilfemaßnahme zu einem bestehenden Playbook erfordert keine Änderung der Lösung selbst.

Note

In den folgenden Anweisungen werden die von der Lösung installierten Ressourcen als Ausgangspunkt verwendet. Konventionell enthalten die meisten Lösungsressourcennamen SHARRund/oder SO0111, um sie leichter auffinden und identifizieren zu können.

Übersicht

Automated Security Response auf AWS Runbooks muss der folgenden Standardbenennung entsprechen:

ASR-*<standard>*-*<version>*-*<control>*

Standard: Die Abkürzung für den Sicherheitsstandard. Dies muss den Standards entsprechen, die von unterstützt werdenSHARR. Es muss „“, „CIS“, „AFSBP“, „PCI“, „NIST“,oder „SC“ sein.

Version: Die Version des Standards. Auch dies muss mit der Version übereinstimmen, die von unterstützt wird, SHARR und der Version in den Suchdaten.

Kontrolle: Die Kontroll-ID des Steuerelements, das repariert werden soll. Dies muss mit den Ergebnisdaten übereinstimmen.

1. Erstellen Sie ein Runbook in dem/den Mitgliedskonto (en).
2. Erstellen Sie eine IAM Rolle in dem/den Mitgliedskonto (en).
3. (Optional) Erstellen Sie eine automatische Behebungsregel im Administratorkonto.

Schritt 1. Erstellen Sie ein Runbook in dem/den Mitgliedskonto (en)

1. Melden Sie sich bei der [AWS Systems Manager Konsole](#) an und erhalten Sie ein Beispiel für das ErgebnisJSON.
2. Erstellen Sie ein Automatisierungs-Runbook, das das Ergebnis behebt. Verwenden Sie auf der Registerkarte „Mein Eigentum“ eines der ASR- Dokumente auf der Registerkarte „Dokumente“ als Ausgangspunkt.
3. AWS Step Functions Im Administratorkonto wird Ihr Runbook ausgeführt. Ihr Runbook muss die Behebungsrolle angeben, damit sie beim Aufrufen des Runbooks übergeben wird.

Schritt 2. Erstellen Sie eine IAM Rolle in den Mitgliedskonten

1. Melden Sie sich an der [AWS Identity and Access Management -Konsole](#) an.
2. Besorgen Sie sich ein Beispiel aus den IAM SO0111-Rollen und erstellen Sie eine neue Rolle. Der Rollename muss mit S00111-Remediate-*<standard>*-*<version>*-*<control>* anfangen. Wenn Sie beispielsweise CIS v1.2.0 Control 5.6 hinzufügen, muss die Rolle S00111-Remediate-CIS-1.2.0-5.6
3. Erstellen Sie anhand des Beispiels eine Rolle mit dem richtigen Umfang, die nur die für die Problembehebung erforderlichen API Aufrufe zulässt.

Zu diesem Zeitpunkt ist Ihre Problembehebung aktiv und kann über die SHARR benutzerdefinierte Aktion in AWS Security Hub automatisiert behoben werden.

Schritt 3: (Optional) Erstellen Sie eine automatische Behebungsregel im Administratorkonto

Automatische (nicht „automatisierte“) Behebung ist die sofortige Ausführung der Behebung, sobald das Ergebnis bei AWS Security Hub eingegangen ist. Bevor Sie diese Option verwenden, sollten Sie die Risiken sorgfältig abwägen.

1. Eine Beispielregel für denselben Sicherheitsstandard finden Sie unter CloudWatch Ereignisse. Der Benennungsstandard für Regeln lautet `standard_control_AutoTrigger`.
2. Kopieren Sie das zu verwendende Ereignismuster aus dem Beispiel.
3. Ändern Sie den `GeneratorId` Wert so, dass er dem `GeneratorId` in Ihrem Ergebnis entsprichtJSON.
4. Speichern und aktivieren Sie die Regel.

Ein neues Playbook hinzufügen

[Laden Sie die Automated Security Response on AWS Solution Playbooks und den Quellcode für die Bereitstellung aus dem GitHub Repository herunter.](#)

Die AWS CloudFormation Ressourcen werden aus [AWS CDK](#) Komponenten erstellt und die Ressourcen enthalten den Playbook-Vorlagencode, mit dem Sie neue Playbooks erstellen und konfigurieren können. [Weitere Informationen zum Einrichten Ihres Projekts und zum Anpassen Ihrer Playbooks finden Sie in der README .md-Datei unter.](#) [GitHub](#)

AWS Systems Manager Parameter speichern

Automated Security Response on AWS verwendet AWS Systems Manager Parameter Store für die Speicherung von Betriebsdaten. Die folgenden Parameter werden im Parameter Store gespeichert:

Name	Wert	Verwenden Sie
/Solutions/S00111/ CMK_REMEDIATION_ARN	AWS KMS Schlüssel, der Daten für FSBP Problembehebungen verschlüsselt	Verschlüsselung von Kundendaten, wie z. B. CloudTrail Protokollen, im Rahmen von Abhilfemaßnahmen
/Solutions/S00111/ CMK_ARN	AWS KMS Schlüssel, der zur Verschlüsselung von Daten verwendet SHARR wird	Verschlüsselung von Lösungsdaten
/Solutions/S00111/ SNS_Topic_ARN	ARNdes SNS Amazon-Themas für die Lösung	Benachrichtigung über Abhilfemaßnahmen
/Solutions/S00111/ SNS_Topic_Config.1	SNSThema für Updates AWS Config	Behebung von Config.1
/Solutions/S00111/ sendAnonymousMetrics	Yes	Erfassung anonymisierter Metriken
/Solutions/S00111/ version	Version der Lösung	
/Solutions/S00111/ <i><security standard long name>/<version></i> / status	enabled	Gibt an, ob der Standard in der Lösung aktiv ist. Ein Standard kann für automatische Problembehebungen deaktiviert werden, indem dieser Wert wie folgt geändert wird disabled

Name	Wert	Verwenden Sie
/Solutions/S00111/ <security standard long name>/shortname	String	Kurzname für den Sicherheitsstandard. Zum Beispiel: 'CIS', AFSBP ", PCI '
/Solutions/S00111/ <security standard long name>/<version> /<control> /remap	String	Wenn ein Steuerelement dieselbe Korrektur wie ein anderes verwendet, führen diese Parameter die Neuordnung durch

SNSAmazon-Thema — Fortschritte bei der Problembhebung

Automated Security Response on AWS erstellt ein SNS Amazon-Thema, SO0111- SHARR _Topic. Dieses Thema wird verwendet, um Updates über den Fortschritt der Problembhebung zu veröffentlichen. Im Folgenden sind die drei möglichen Benachrichtigungen aufgeführt, die zu diesem Thema gesendet werden können.

```
Remediation queued for <standard> control <control_ID> in account <account_ID>
```

```
Remediation failed for <standard> control <control_ID> in account <account_ID>
```

```
<control_ID> remediation was successfully invoke via AWS Systems Manager in  
account <account_ID>
```

Dies ist die Abschlussnachricht. Es weist darauf hin, dass die Wiederherstellung ohne Fehler abgeschlossen wurde. Der endgültige Test für eine erfolgreiche Wiederherstellung ist jedoch die AWS Konfigurationsprüfung und/oder die manuelle Validierung.

Ein Themenabonnement SNS filtern

[Richtlinien SNS für Amazon-Abonnementfilter:](#)

1. Navigieren Sie zum Abonnement des SNS Themas.
2. Wählen Sie unter Abonnementfilterrichtlinie die Option „Bearbeiten“ aus.

3. Erweitern Sie „Abonnementfilterrichtlinie“ und aktivieren Sie die Option „Abonnementfilterrichtlinie“, um Filter zu aktivieren.
4. Wählen Sie den Bereich „Nachrichtentext“ aus.
5. Fügen Sie Ihre Richtlinie dem JSON Editor hinzu.
6. Speichern Sie die Änderungen.

Beispielrichtlinien:

Nach Konto filtern

```
{
  "finding": {
    "account": [
      "111111111111",
      "222222222222"
    ]
  }
}
```

Nach Fehlern filtern

```
{
  "severity": ["ERROR"]
}
```

Nach Steuerelementen filtern

```
{
  "finding": {
    "standard_control": ["S3.9", "S3.6"]
  }
}
```

SNSAmazon-Thema — CloudWatch Alarme

Diese Lösung erstellt ein SNS Amazon-Thema, `S00111-ASR_Alarm_Topic`. Dieses Thema wird verwendet, um Alarmmeldungen zu veröffentlichen.

Einzelheiten zu allen Alarmen, die in den ALARM Status wechseln, werden an dieses Thema gesendet.

Runbook bei Konfigurationsergebnissen starten

Diese Lösung kann Runbooks auf der Grundlage benutzerdefinierter AWS Config Ergebnisse initiieren. Um dies zu tun, müssen Sie:

1. Suchen Sie den AWS Config Regelnamen, den Sie korrigieren möchten. Dies kann entweder in AWS Config oder in dem Ergebnis gefunden werden, das Security Hub für diese Regel generiert.
2. Navigieren Sie zu AWS Systems Manager Parameter Store und wählen Sie Parameter erstellen aus.
3. Der Name Ihrer Regel sollte lauten `/Solutions/S00111/Rule name from Step 1`
4. Der Wert sollte wie folgt formatiert sein:

```
{  
  
"RunbookName": "Name of SSM runbook",  
  
"RunbookRole": "Role that Orchestrator will assume"  
}
```

5. RunbookName ist ein Pflichtfeld und ist das Runbook, das ausgeführt wird, wenn Sie diese Konfigurationsregel korrigieren. RunbookRole ist die Rolle, die der Orchestrator bei der Ausführung dieser Rolle übernimmt. Es ist kein Pflichtfeld, und wenn es weggelassen wird, verwendet der Orchestrator standardmäßig die Mitgliedsrolle des Kontos.
6. Sobald dies eingerichtet ist, können Sie Ihre Konfigurationsregel mithilfe der benutzerdefinierten Aktion „Reparieren mitASR“ auf dem Security Hub korrigieren.

Referenz

Dieser Abschnitt enthält Informationen zu einer optionalen Funktion zum Sammeln einzigartiger Metriken für diese Lösung, Verweise auf verwandte Ressourcen und eine Liste der Entwickler, die zu dieser Lösung beigetragen haben.

Anonymisierte Datenerfassung

Diese Lösung beinhaltet eine Option zum Senden anonymisierter Betriebskennzahlen an AWS. Wir verwenden diese Daten, um besser zu verstehen, wie Kunden diese Lösung und die damit verbundenen Services und Produkte nutzen. Wenn diese Option aktiviert ist, werden die folgenden Informationen gesammelt und gesendet an AWS:

- Lösungs-ID — Die AWS Lösungs-ID
- Eindeutige ID (UUID) — Zufällig generierte, eindeutige Kennung für jede AWS Security Hub Reaktions- und Behebungsbereitstellung
- Zeitstempel — Zeitstempel für die Datenerfassung
- Instanzdaten — Informationen zu dieser Stack-Bereitstellung
- CloudWatchMetricsDashboardEnabled— "Yes" wenn CloudWatch Metriken und Dashboard während der Bereitstellung aktiviert sind
- Status — Bereitstellungsstatus (Lösung bestanden oder fehlgeschlagen) oder (Problembehebung bestanden oder fehlgeschlagen)
- Fehlermeldung — Die allgemeine Fehlermeldung im Statusfeld
- Generator_ID — Informationen zur Security Hub Hub-Regel
- Typ — Art und Name der Behebung
- productArn- Die Region, in der Security Hub eingesetzt wird
- finding_triggered_by — Die Art der durchgeführten Behebung (benutzerdefinierte Aktion oder automatisierter Auslöser)

AWS besitzt die im Rahmen dieser Umfrage gesammelten Daten. Die Datenerfassung unterliegt der [AWS Datenschutzerklärung](#). Um diese Funktion zu deaktivieren, führen Sie die folgenden Schritte aus, bevor Sie die AWS CloudFormation Vorlage starten.

1. Laden Sie die [AWS CloudFormation Vorlage](#) auf Ihre lokale Festplatte herunter.

2. Öffnen Sie die AWS CloudFormation Vorlage mit einem Texteditor.
3. Ändern Sie den Abschnitt zur AWS CloudFormation Vorlagenzuweisung von:

```
Mappings:
  Solution:
    Data:
      SendAnonymizedUsageData: 'Yes'
```

auf:

```
Mappings:
  Solution:
    Data:
      SendAnonymizedUsageData: 'No'
```

4. Melden Sie sich an der [AWS CloudFormation -Konsole](#) an.
5. Wählen Sie Stapel erstellen aus.
6. Wählen Sie auf der Seite Stack erstellen im Abschnitt Vorlage angeben die Option Eine Vorlagendatei hochladen aus.
7. Wählen Sie unter Vorlagendatei hochladen die Option Datei auswählen und wählen Sie die bearbeitete Vorlage von Ihrem lokalen Laufwerk aus.
8. Wählen Sie Weiter und folgen Sie den Schritten unter [Stack starten](#) im Abschnitt Automatisierte Bereitstellung dieses Handbuchs.

Zugehörige Ressourcen

- [Automatisierte Reaktion und Problembeseitigung mit AWS Security Hub](#)
- [CIS Benchmarks der Amazon Web Services Foundations, Version 1.2.0](#)
- [AWS Foundational Security Best Practices-Standard](#)
- [Datensicherheitsstandard der Zahlungskartenbranche \(\) PCI DSS](#)
- [Nationales Institut für Standards und Technologie \(NIST\) SP 800-53 Rev. 5](#)

Mitwirkende

Die folgenden Personen haben zu diesem Dokument beigetragen:

- Mike O'Brien
- Nikhil Reddy
- Chandini Penmetsa
- Chaitanya Deolankar
- Max Granat
- Tim Mekari
- Aaron Schütter
- Andrew Yankowski
- Josh Moss
- Ryan Garay
- Thiemo Belmega

Überarbeitungen

Datum	Änderung
August 2020	Erstversion
Oktober 2020	Zusätzliche Informationen zur Fehlerbehebung wurden zu Anhang C hinzugefügt.
November 2020	Bereitstellungsanweisungen für China Regionen hinzugefügt; aktualisierte Anweisungen zur Lösungsbereitstellung für das Security Hub-Administratorkonto; weitere Informationen finden Sie in der CHANGELOG.md-Datei im GitHub Repository.
April 2021	Version v1.2.0: Neue Playbook-Architektur und neue FSBP Abhilfemaßnahmen hinzugefügt. Weitere Informationen finden Sie in der CHANGELOG.md-Datei im Repository. GitHub
Mai 2021	Version v1.2.1: Bugfix für ein Problem, das EC2 2.2 und EC2 1.7 betrifft. Weitere Informationen finden Sie in der CHANGELOG.md-Datei im Repository. GitHub
August 2021	Version v1.3.0: Playbook PCI DSS v3.2.1 hinzugefügt. 17 neue Abhilfemaßnahmen wurden zu v1.2.0 hinzugefügt. CIS Vier neue Abhilfemaßnahmen wurden hinzugefügt. FSBP Umgestellt CIS, um eine neue Playbook-Architektur zu verwenden, die auf SSM Runbooks basiert. Es wurden Anweisungen zur Erweiterung vorhandener Playbooks um vom Kunden definierte Korrekturen hinzugefügt. Weitere Informationen finden Sie in der CHANGELOG.md-Datei im Repository. GitHub

Datum	Änderung
September 2021	Version v1.3.1: CreateLogMetricFilterAndAlarm.py wurde dahingehend geändert, dass Aktionen aktiviert werden, SNS Benachrichtigung hinzugefügt S00111-SHARR-LocalAlarmNotification wird. Die Problembehebung in Version CIS 2.8 wurde geändert, sodass sie dem neuen Datenformat für Ergebnisse entspricht. Weitere Informationen finden Sie in der CHANGELOG.md-Datei im GitHub Repository.
November 2021	Version v1.3.2: Fehlerkorrekturen für die CIS v1.2.0-Steuerelemente 3.1 - 3.14. Weitere Informationen finden Sie in der CHANGELOG.md-Datei im Repository. GitHub
Dezember 2021	Version v1.4.0: Die Lösung kann jetzt mit bereitgestellt werden. StackSets Zusätzlich zur kontenübergreifenden Problembehebung wird jetzt auch regionsübergreifende Problembehebung unterstützt. IAMRollen von Mitglieds konten werden jetzt beibehalten, wenn der Stack entfernt wird. Weitere Informationen finden Sie in der CHANGELOG.md-Datei im GitHub Repository.
Januar 2022	Version v1.4.1: Fehlerkorrekturen. Weitere Informationen finden Sie in der CHANGELOG.md-Datei im GitHub Repository.
Januar 2022	Version v1.4.2: Fehlerkorrekturen. Weitere Informationen finden Sie in der CHANGELOG.md-Datei im GitHub Repository.

Datum	Änderung
Juni 2022	Version v1.5.0: Zusätzliche Abhilfemaßnahmen. Weitere Informationen finden Sie in der CHANGELOG.md-Datei im Repository. GitHub
Dezember 2022	Version 1.5.1 Änderungen zur Umstellung der SSM Dokumentenerstellung von Custom Resource Lambda auf. CfnDocument Das Präfix für die SSM Dokumentnamen wurde aktualisiert und beginnt nun mit ASR statt mit. SHARR Weitere Informationen finden Sie in der CHANGELOG.md-Datei im GitHub Repository.
März 2023	Version 2.0.0: Unterstützung für Sicherheitskontrollen und CIS v1.4.0-Standards hinzugefügt, fünf neue Korrekturen an Standards, eine neue Anpassung an die FSBP CIS v1.2.0-Standards, die AppRegistry Integration des Servicekatalogs und zusätzliche Schutzmaßnahmen zur Vermeidung von Bereitstellungsfehlern aufgrund von Dokumentendrosselung. SSM Weitere Informationen finden Sie in der .md-Datei im Repository. CHANGELOG GitHub
April 2023	Version 2.0.1: Die Auswirkungen, die durch die neuen Standardeinstellungen für S3 Object Ownership (ACLsdeaktiviert) für alle neuen S3-Buckets verursacht wurden, wurden gemildert. Weitere Informationen finden Sie in der CHANGELOG.md-Datei im Repository. GitHub

Datum	Änderung
Mai 2023	Aktualisierung der Dokumentation: Aktualisierte Well-Architected-Definitionen, zusätzliche Hinweise zur Bereitstellung der einzelnen Stacks, zusätzliche Version zur Problembekämpfung mit spezifischen Problemlösungen und aktualisierte Codebeispiele in der Benachrichtigung. SNS
Juli 2023	Aktualisierung der Dokumentation: Das Architekturdiagramm und die Lösungskomponenten im Workflow wurden aktualisiert.
Oktober 2023	Version 2.0.2: Aktualisierte Paketversionen zur Behebung von Sicherheitslücken. Weitere Informationen finden Sie in der CHANGELOG .md-Datei im GitHub Repository.
November 2023	Aktualisierung der Dokumentation: Mit der Lösung verknüpfte Kosten-Tags bestätigen zum AppRegistry Abschnitt „Lösung mit AWS Service Catalog überwachen“ hinzugefügt.
März 2024	Version 2.1.0: Unterstützung für den NIST Standard hinzugefügt, 17 neue Abhilfemaßnahmen zu FSBP Standards hinzugefügt, CloudWatch Dashboard für die Überwachungslösung hinzugefügt, Drosselungsprozedur zur Architektur hinzugefügt, Unterstützung für anpassbare Eingabeparameter in Security Hub hinzugefügt und Unterstützung für die Korrektur von Config-Ergebnissen hinzugefügt. Weitere Informationen finden Sie in der CHANGELOG .md-Datei im Repository . GitHub

Datum	Änderung
April 2024	Version 2.1.1: Die Dokumentation wurde auf die Reihenfolge der CloudFormation Parameter und die Standardwerte aktualisiert. Verweise auf den NIST Standard hinzugefügt. Es wurden Informationen zu Quoten für den EventBridge Regeldienst hinzugefügt. Weitere Informationen finden Sie in der CHANGELOG.md-Datei im GitHub Repository.
Juni 2024	Version 2.1.2: AppRegistry Für bestimmte Playbooks deaktiviert, um Fehler bei der Aktualisierung der Lösung zu vermeiden . Weitere Informationen finden Sie in der CHANGELOG.md-Datei im Repository. GitHub
September 2024	Version 2.1.3: Es wurde ein Problem in den Behebungsskripten für EC2 .18 und EC2 .19 behoben, bei dem Sicherheitsgruppenregeln mit dem Wert -1 IpProtocol fälschlicherweise ignoriert wurden. Alle Python-Laufzeiten in SSM Behebungsdokumenten wurden von Python 3.8 auf Python 3.11 aktualisiert. Weitere Informationen finden Sie in der CHANGELOG.md-Datei im Repository. GitHub
November 2024	Version 2.1.4: Python-Laufzeiten in allen Control-Runbooks wurden von Python 3.8 auf Python 3.11 aktualisiert. Weitere Informationen finden Sie in der CHANGELOG.md-Datei im Repository . GitHub

Datum	Änderung
Dezember 2024	Version 2.2.0: Integration des Ticketsystems, CloudTrail Aktionsprotokoll und CIS 3.0.0-Playbook hinzugefügt. Verbessertes Dashboard und Benachrichtigungen. Weitere Informationen finden Sie in der CHANGELOG.md-Datei im GitHub Repository.

Hinweise

Kunden sind dafür verantwortlich, Ihre eigene unabhängige Bewertung der Informationen in diesem Dokument vorzunehmen. Dieses Dokument: (a) dient nur zu Informationszwecken, (b) stellt AWS aktuelle Produktangebote und Praktiken dar, die ohne vorherige Ankündigung geändert werden können, und (c) stellt keine Verpflichtungen oder Zusicherungen von AWS und seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern dar. AWS Produkte oder Dienstleistungen werden „wie sie sind“ ohne ausdrückliche oder stillschweigende Garantien, Zusicherungen oder Bedingungen jeglicher Art bereitgestellt. AWS Die Verantwortlichkeiten und Verbindlichkeiten gegenüber seinen Kunden werden durch AWS Vereinbarungen geregelt, und dieses Dokument ist weder Teil einer Vereinbarung zwischen AWS und seinen Kunden noch ändert es diese.

Automated Security Response on AWS ist unter den Bedingungen der Apache License Version 2.0 lizenziert, die bei [The Apache Software Foundation](https://www.apache.org/licenses/LICENSE-2.0) erhältlich ist.

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.