aws

GuardDuty Amazon-Benutzerhandbuch

Amazon GuardDuty

Amazon GuardDuty: GuardDuty Amazon-Benutzerhandbuch

Table of Contents

Was ist Amazon GuardDuty?

Amazon GuardDuty ist ein Service zur Bedrohungserkennung, der Ihre AWS Umgebung kontinuierlich auf potenzielle Sicherheitsrisiken überwacht. GuardDuty analysiert und verarbeitetGrundlegende Datenquellen, z. B. AWS CloudTrail Verwaltungsereignisse, AWS CloudTrail Ereignisprotokolle, VPC-Flussprotokolle (von Amazon EC2 EC2-Instances) und DNS-Protokolle. GuardDuty bietet auch Überwachungsprotokolle und Ereignisse von anderen AWS Diensten. Zu diesen Quellen gehören EKS-Auditprotokolle, RDS-Anmeldeaktivitäten, S3-Protokolle, EBS-Volumes, Runtime-Überwachung und Lambda-Netzwerkaktivitätsprotokolle. GuardDutyfasst diese Protokoll- und Ereignisquellen unter dem Begriff Funktionen zusammen.

GuardDuty verwendet Feeds mit Bedrohungsinformationen wie Listen bösartiger IP-Adressen und Domänen sowie Modelle für maschinelles Lernen (ML), um unerwartete, potenziell nicht autorisierte und bösartige Aktivitäten in Ihrer AWS Umgebung zu identifizieren. Dazu gehören Probleme wie die Eskalation von Rechten, die Verwendung offengelegter Anmeldeinformationen oder die Kommunikation mit bösartigen IP-Adressen und Domänen, das Vorhandensein von Malware auf Ihren Amazon EC2 EC2-Instances und Container-Workloads oder die Entdeckung ungewöhnlicher Muster von Anmeldeereignissen in Ihrer Datenbank.

GuardDuty Kann beispielsweise potenziell gefährdete EC2-Instances und Container-Workloads erkennen, die Malware bereitstellen oder Bitcoin minen. Es überwacht auch das Verhalten AWS beim Kontozugriff auf Anzeichen einer möglichen Gefährdung, wie z. B. unautorisierte Infrastrukturbereitstellungen — also Instanzen, die in einer Region bereitgestellt werden, die noch nie genutzt wurde, oder ungewöhnliche API-Aufrufe — die Passwortrichtlinie wurde geändert, um die Passwortstärke zu verringern.

Wenn diese Option aktiviert ist, GuardDuty bietet sie Einblick in den Sicherheitsstatus Ihrer AWS Umgebung. Wenn es ein potenzielles Sicherheitsrisiko identifiziert, generiert es einen Befund und stellt weitere Details bereit. Sie können Amazon auch so einrichten EventBridge , dass es Benachrichtigungen erhält, wenn ein Ergebnis GuardDuty generiert wird. GuardDuty empfiehlt außerdem Schritte zur Behebung der Hinweise auf Sicherheitsprobleme in Ihrer Umgebung.

Sie können die generierten Ergebnisse in einen Amazon Simple Storage Service (Amazon S3) -Bucket exportieren. GuardDuty lässt sich auch in andere AWS sicherheitsrelevante Dienste wie AWS Security Hub Amazon Detective integrieren, die Sie bei der Analyse und Untersuchung der Sicherheitstrends in Ihrer Umgebung weiter unterstützen können.

Verwenden GuardDuty

Sie können es GuardDuty auf eine der folgenden Arten verwenden:

GuardDuty Konsole

https://console.aws.amazon.com/guardduty

Die Konsole ist eine browserbasierte Oberfläche für den Zugriff und die Verwendung GuardDuty. Die GuardDuty Konsole bietet Zugriff auf Ihr GuardDuty Konto, Ihre Daten und Ressourcen.

AWS Befehlszeilentools

Mit AWS Befehlszeilentools können Sie Befehle an der Befehlszeile Ihres Systems ausgeben, um GuardDuty Aufgaben und AWS Aufgaben auszuführen. Die Befehlszeilen-Tools können auch beim Erstellen von Skripts für Aufgaben hilfreich sein.

Informationen zur Installation und Verwendung AWS CLI finden Sie im AWS Command Line Interface Benutzerhandbuch. Die verfügbaren AWS CLI Befehle für finden Sie GuardDuty unter CLI-Befehlsreferenz.

GuardDuty HTTPS-API

Sie können mithilfe der GuardDuty HTTPS-API AWS programmgesteuert darauf zugreifen GuardDuty , sodass Sie HTTPS-Anfragen direkt an den Dienst senden können. Weitere Informationen finden Sie in der GuardDuty API-Referenz.

AWS SDKs

AWS bietet Software Development Kits (SDKs), die aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen (Java, Python, Ruby, .NET, iOS, Android und mehr) bestehen. Die SDKs bieten eine bequeme Möglichkeit, programmatischen Zugriff auf zu erstellen. GuardDuty Weitere Informationen über die AWS -SDKs, das Herunterladen und die Installation finden Sie unter Tools für Amazon Web Services.

Preisgestaltung für GuardDuty

Bei der ersten Nutzung gibt es GuardDuty für jedes AWS Konto pro AWS Region eine kostenlose 30-Tage-Testversion. Weitere Informationen finden Sie unter -Preisgestaltung.

Unterstützte Regionen AWS

Informationen zu AWS Regionen, in denen Sie die Option aktivieren können GuardDuty, finden Sie unterRegionen und Endpunkte.

Erste Schritte mit GuardDuty

Dieses Tutorial bietet eine praktische Einführung in. GuardDuty Die Mindestanforderungen für die Aktivierung GuardDuty als eigenständiges Konto oder als GuardDuty Administrator mit AWS Organizations werden in Schritt 1 behandelt. Die Schritte 2 bis 5 behandeln die Verwendung zusätzlicher Funktionen, die von empfohlen werden GuardDuty , um das Beste aus Ihren Ergebnissen herauszuholen.

Themen

Bevor Sie beginnen

GuardDuty ist ein Dienst zur Bedrohungserkennung, der Grundlegende Datenquellen beispielsweise AWS CloudTrail Ereignisprotokolle, AWS CloudTrail Verwaltungsereignisse, Amazon VPC Flow Logs und DNS-Protokolle überwacht. GuardDuty analysiert auch Funktionen, die mit seinen Schutztypen verknüpft sind, nur wenn Sie sie separat aktivieren. Zu den Funktionen gehören Kubernetes-Prüfungsprotokolle, RDS-Anmeldeaktivitäten, S3-Protokolle, EBS-Volumes, Laufzeit-Überwachung und Lambda-Netzwerkaktivitätsprotokolle. Durch die Verwendung dieser Datenquellen und Funktionen (sofern aktiviert) werden Sicherheitsergebnisse für Ihr Konto GuardDuty generiert.

Nach der Aktivierung beginnt GuardDuty es mit der Überwachung Ihrer Umgebung. Sie können GuardDuty die Option für jedes Konto in jeder Region jederzeit deaktivieren. Dadurch werden die grundlegenden Datenquellen und alle Funktionen, die separat aktiviert wurden, nicht mehr GuardDuty verarbeitet.

Sie müssen keine der Grundlegende Datenquellen explizit aktivieren. Amazon GuardDuty bezieht unabhängige Datenströme direkt von diesen Diensten. Für ein neues GuardDuty Konto sind alle verfügbaren Schutzarten, die in einem unterstützt werden, AWS-Region standardmäßig aktiviert und in der 30-tägigen kostenlosen Testphase enthalten. Sie können einen oder alle von ihnen deaktivieren. Wenn Sie bereits GuardDuty Kunde sind, können Sie wählen, ob Sie einige oder

alle Schutzpläne aktivieren möchten, die in Ihrem AWS-Region Paket verfügbar sind. Weitere Informationen finden Sie unter Zu den einzelnen Schutztypen gehörende Funktionen in GuardDuty.

Beachten Sie bei der Aktivierung GuardDuty die folgenden Punkte:

- GuardDuty ist ein regionaler Dienst, was bedeutet, dass alle Konfigurationsverfahren, die Sie auf dieser Seite ausführen, in jeder Region, mit der Sie überwachen möchten, wiederholt werden müssen GuardDuty.

  Wir empfehlen dringend, die Aktivierung GuardDuty in allen unterstützten AWS Regionen durchzuführen. Auf diese Weise können GuardDuty auch in Regionen, die Sie nicht aktiv nutzen, Erkenntnisse über unbefugte oder ungewöhnliche Aktivitäten generiert werden. Dies ermöglicht auch GuardDuty die Überwachung von AWS CloudTrail Ereignissen für globale AWS Dienste wie IAM. Wenn diese Option nicht in allen unterstützten Regionen aktiviert GuardDuty ist, ist ihre Fähigkeit zur Erkennung von Aktivitäten, die globale Dienste betreffen, eingeschränkt. Eine vollständige Liste der Regionen, in denen GuardDuty es verfügbar ist, finden Sie unterRegionen und Endpunkte.
- Jeder Benutzer mit Administratorrechten in einem AWS Konto kann diese Option aktivieren GuardDuty. Gemäß der bewährten Sicherheitsmethode der geringsten Rechte wird jedoch empfohlen, eine IAM-Rolle, einen Benutzer oder eine Gruppe zu erstellen, die GuardDuty speziell verwaltet werden soll. Informationen zu den für die Aktivierung erforderlichen Berechtigungen GuardDuty finden Sie unterErforderliche Berechtigungen zum Aktivieren von GuardDuty.
- Wenn Sie sie GuardDuty zum ersten Mal in einer beliebigen AWS-Region Region aktivieren, werden standardmäßig auch alle verfügbaren Schutztypen aktiviert, die in dieser Region unterstützt werden, einschließlich Malware-Schutz. GuardDuty erstellt eine mit dem Dienst verknüpfte Rolle für Ihr Konto mit dem Namen. `AWSServiceRoleForAmazonGuardDuty` Diese Rolle umfasst die Berechtigungen und Vertrauensrichtlinien, die es ermöglichen, Ereignisse direkt aus GuardDuty dem zu verarbeiten und zu analysieren, Grundlegende Datenquellen um daraus Sicherheitsresultate zu generieren. Malware Protection erstellt für Ihr Konto eine weitere serviceverknüpfte Rolle namens `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Diese Rolle umfasst die Berechtigungen und Vertrauensrichtlinien, die es Malware Protection ermöglichen, Scans ohne Agenten durchzuführen, um Malware in Ihrem GuardDuty Konto zu erkennen. Sie ermöglicht es GuardDuty , einen EBS-Volume-Snapshot in Ihrem Konto zu erstellen und diesen Snapshot mit dem GuardDuty Dienstkonto zu teilen. Weitere Informationen finden Sie unter Mit dem Dienst verknüpfte Rollenberechtigungen für GuardDuty. Weitere Informationen zu serviceverknüpften Rollen finden Sie unter Verwenden serviceverknüpfter Rollen.

- Wenn Sie Ihr Konto GuardDuty zum ersten Mal in einer Region aktivieren, wird Ihr AWS Konto automatisch für eine GuardDuty kostenlose 30-Tage-Testversion für diese Region registriert.

Schritt 1: Amazon aktivieren GuardDuty

Der erste Schritt zur Verwendung GuardDuty besteht darin, es in Ihrem Konto zu aktivieren. Nach der Aktivierung GuardDuty wird sofort mit der Überwachung auf Sicherheitsbedrohungen in der aktuellen Region begonnen.

Wenn Sie die GuardDuty Ergebnisse für andere Konten innerhalb Ihrer Organisation als GuardDuty Administrator verwalten möchten, müssen Sie Mitgliedskonten hinzufügen und diese ebenfalls aktivieren GuardDuty . Wählen Sie eine Option aus, um zu erfahren, wie Sie sie GuardDuty für Ihre Umgebung aktivieren können.

Standalone account environment

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/
2. Wählen Sie Get Started.
3. Wählen Sie „Aktivieren GuardDuty“.

Multi-account environment

> **Important**
>
> Voraussetzung für diesen Prozess ist, dass Sie derselben Organisation angehören wie alle Konten, die Sie verwalten möchten, und Zugriff auf das AWS Organizations Verwaltungskonto haben, um einen Administrator GuardDuty innerhalb Ihrer Organisation delegieren zu können. Für die Delegierung eines Administrators sind möglicherweise zusätzliche Berechtigungen erforderlich. Weitere Informationen finden Sie unter Für die Benennung eines delegierten GuardDuty Administratorkontos sind Berechtigungen erforderlich.

Um ein GuardDuty delegiertes Administratorkonto zu bestimmen

1. Öffnen Sie die AWS Organizations Konsole unter https://console.aws.amazon.com/organizations/ mit dem Verwaltungskonto.

2. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Ist in Ihrem Konto GuardDuty bereits aktiviert?

   - Falls GuardDuty es noch nicht aktiviert ist, können Sie Erste Schritte auswählen und dann auf der Seite Willkommen GuardDuty bei einen GuardDuty delegierten Administrator benennen.
   - Wenn diese Option aktiviert GuardDuty ist, können Sie auf der Seite „Einstellungen“ einen GuardDuty delegierten Administrator festlegen.

3. Geben Sie die zwölfstellige AWS Konto-ID des Kontos ein, das Sie als delegierten Administrator für die Organisation bestimmen möchten, und wählen Sie GuardDuty Delegieren aus.

   > **Note**
   >
   > Falls dies noch nicht aktiviert GuardDuty ist, wird durch die Benennung eines delegierten Administrators die Aktivierung GuardDuty für dieses Konto in Ihrer aktuellen Region aktiviert.

So fügen Sie Mitgliedskonten hinzu

Dieses Verfahren umfasst das Hinzufügen von Mitgliederkonten zu einem GuardDuty delegierten Administratorkonto durch. AWS Organizations Es besteht auch die Möglichkeit, Mitglieder auf Einladung hinzuzufügen. Weitere Informationen zu beiden Methoden zum Zuordnen von Mitgliedern finden Sie GuardDuty unter. Verwaltung mehrerer Konten bei Amazon GuardDuty

1. Melden Sie sich im delegierten Administratorkonto an
2. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
3. Wählen Sie im Navigationsbereich Settings (Einstellungen) und dann Accounts (Konten) aus.

   In der Kontentabelle werden alle Konten in der Organisation angezeigt.

4. Wählen Sie die Konten aus, die Sie als Mitglieder hinzufügen möchten, indem Sie das Kontrollkästchen neben der Konto-ID aktivieren. Wählen Sie dann im Menü Aktion die Option Mitglied hinzufügen.

> **Tip**
>
> Sie können das Hinzufügen neuer Konten als Mitglieder mit dem Feature Automatisch aktivieren automatisieren. Dies gilt jedoch nur für Konten, die Ihrer Organisation beitreten, nachdem das Feature aktiviert wurde.

Schritt 2: Beispiel-Erkenntnisse generieren und die grundlegenden Abläufe erkunden

Wenn ein Sicherheitsproblem GuardDuty entdeckt wird, wird ein Befund generiert. Ein GuardDuty Befund ist ein Datensatz, der Details zu diesem speziellen Sicherheitsproblem enthält. Die Einzelheiten der Erkenntnis können Ihnen bei der Untersuchung des Problems helfen.

GuardDuty unterstützt die Generierung von Stichprobenergebnissen mit Platzhalterwerten, anhand derer Sie die GuardDuty Funktionalität testen und sich mit den Ergebnissen vertraut machen können, bevor Sie auf ein echtes Sicherheitsproblem reagieren müssen, das von entdeckt wurde. GuardDuty Folgen Sie der nachstehenden Anleitung, um Beispielergebnisse für jeden Befundtyp zu generieren GuardDuty, der unter verfügbar ist. Weitere Möglichkeiten zur Generierung von Stichprobenergebnissen, einschließlich der Generierung eines simulierten Sicherheitsereignisses in Ihrem Konto, finden Sie unter. Beispielergebnisse

So erstellen und untersuchen Sie Beispiel-Erkenntnisse

1. Wählen Sie im Navigationsbereich Settings (Einstellungen).
2. Klicken Sie auf der Seite Settings unter Sample findings auf Generate sample findings.
3. Wählen Sie im Navigationsbereich Zusammenfassung aus, um die in Ihrer AWS Umgebung generierten Erkenntnisse zu den Ergebnissen anzuzeigen. Weitere Informationen zu den Komponenten des Übersichts-Dashboards finden Sie unter Übersichts-Dashboard.
4. Wählen Sie im Navigationsbereich Findings aus. Die Beispiel-Erkenntnisse werden auf der Seite Aktuelle Erkenntnisse mit dem Präfix [SAMPLE] angezeigt.
5. Wählen Sie eine Erkenntnis aus der Liste aus, um Details zur Erkenntnis anzuzeigen.

    - Sie können die verschiedenen Informationsfelder überprüfen, die im Bereich mit den Erkenntnisdetails verfügbar sind. Verschiedene Arten von Erkenntnissen können unterschiedliche Felder haben. Weitere Informationen zu den verfügbaren Feldern für alle

Erkenntnistypen finden Sie unter Erkenntnisdetails. In der Detailansicht können Sie die folgenden Aktionen durchführen:

- Wählen Sie oben im Bereich die Erkenntnis-ID aus, um die vollständigen JSON-Details für die Erkenntnis zu öffnen. Die vollständige JSON-Datei kann auch von dieser Ansicht heruntergeladen werden. Das JSON enthält einige zusätzliche Informationen, die nicht in der Konsolenansicht enthalten sind. Es ist das Format, das von anderen Tools und Services aufgenommen werden kann.
- Sehen Sie sich den Abschnitt Betroffene Ressource an. Bei einem echten Ergebnis helfen Ihnen die Informationen hier dabei, eine Ressource in Ihrem Konto zu identifizieren, die untersucht werden sollte, und sie enthalten Links zu den entsprechenden AWS Management Console Ressourcen, die umsetzbar sind.
- Wählen Sie das + oder - beim Lupensymbol, um einen inklusiven oder exklusiven Filter für dieses Detail zu erstellen. Weitere Informationen zu Filtern finden Sie unter Filtern von Ergebnissen.

6. Archivieren Sie all Ihre Beispiel-Erkenntnisse

   a. Wählen Sie alle Erkenntnisse aus, indem Sie das Kontrollkästchen oben in der Liste aktivieren.

   b. Deaktivieren Sie alle Erkenntnisse, die Sie behalten möchten.

   c. Wählen Sie das Menü Aktionen und dann Archivieren, um die Beispiel-Erkenntnisse auszublenden.

> **Note**
>
> Um die archivierten Erkenntnisse anzuzeigen, wählen Sie Aktuell und dann Archiviert, um zur Erkenntnisansicht zu wechseln.

Schritt 3: Konfigurieren Sie den Export von GuardDuty Ergebnissen in einen Amazon S3 S3-Bucket

GuardDuty empfiehlt, Einstellungen für den Export von Ergebnissen zu konfigurieren, da Sie so Ihre Ergebnisse in einen S3-Bucket exportieren können, um sie nach Ablauf der Aufbewahrungsfrist von GuardDuty 90 Tagen auf unbestimmte Zeit zu speichern. Auf diese Weise können Sie Aufzeichnungen über die Ergebnisse führen oder Probleme in Ihrer AWS Umgebung im Laufe der

Zeit verfolgen. Der hier beschriebene Prozess führt Sie durch die Einrichtung eines neuen S3-Buckets und die Erstellung eines neuen KMS-Schlüssels zur Verschlüsselung der Erkenntnisse von der Konsole aus. Weitere Informationen dazu, wie Sie Ihren eigenen vorhandenen Bucket oder einen Bucket in einem anderen Konto verwenden können, finden Sie unter Exportieren von Erkenntnissen.

So konfigurieren Sie die Option zum Export von Erkenntnissen an S3

1. Um die Ergebnisse zu verschlüsseln, benötigen Sie einen KMS-Schlüssel mit einer Richtlinie, die die Verwendung dieses Schlüssels für die Verschlüsselung ermöglicht GuardDuty . Die folgenden Schritte helfen Ihnen beim Erstellen eines neuen KMS-Schlüssels. Wenn Sie einen KMS-Schlüssel von einem anderen Konto verwenden, müssen Sie die Schlüsselrichtlinie anwenden, indem Sie sich bei dem Konto anmelden AWS-Konto , dem der Schlüssel gehört. Die Region Ihres KMS-Schlüssels und Ihres S3-Buckets muss dieselbe sein. Sie können jedoch dasselbe Bucket und Schlüsselpaar für jede Region verwenden, aus der Sie Erkenntnisse exportieren möchten.

   a. Öffnen Sie die AWS KMS Konsole unter https://console.aws.amazon.com/kms.

   b. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.

   c. Klicken Sie im Navigationsbereich auf Kundenverwaltete Schlüssel.

   d. Klicken Sie auf Create key.

   e. Wählen Sie unter Schlüsseltyp die Option Symmetrisch und dann Weiter.

      > **Note**
      >
      > Informationen zum Erstellen Ihres KMS-Schlüssels finden Sie unter Erstellen von Schlüsseln im Entwicklerhandbuch für AWS Key Management Service .

   f. Geben Sie einen Alias für Ihren Schlüssel ein und wählen Sie dann Weiter aus.

   g. Wählen Sie Weiter und dann erneut Weiter, um die standardmäßigen Verwaltungs- und Nutzungsberechtigungen zu akzeptieren.

   h. Nachdem Sie die Konfiguration überprüft haben, wählen Sie Fertigstellen, um den Schlüssel zu erstellen.

   i. Wählen Sie auf der Seite Vom Kunden verwaltete Schlüssel Ihren Schlüsselalias aus.

   j. Wählen Sie im Abschnitt Schlüsselrichtlinie die Option Zur Richtlinienansicht wechseln aus.

k. Wählen Sie Bearbeiten und fügen Sie Ihrem KMS-Schlüssel die folgende Schlüsselrichtlinie hinzu, um GuardDuty Zugriff auf Ihren Schlüssel zu gewähren. Mit dieser Anweisung können GuardDuty Sie nur den Schlüssel verwenden, zu dem Sie diese Richtlinie hinzufügen. Stellen Sie beim Bearbeiten der Schlüsselrichtlinie sicher, dass die JSON-Syntax gültig ist. Wenn Sie die Anweisung vor der finalen Anweisung hinzufügen, müssen Sie nach der schließenden Klammer ein Komma hinzufügen.

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "arn:aws:kms:Region1:444455556666:key/KMSKeyId",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:111122223333:detector/SourceDetectorID"
        }
    }
}
```

Ersetzen Sie *Region1* durch die Region Ihres KMS-Schlüssels. Ersetzen Sie *444455556666* durch den, dem der AWS-Konto KMS-Schlüssel gehört. Ersetzen Sie *KMS KeyId* durch die Schlüssel-ID des KMS-Schlüssels, den Sie für die Verschlüsselung ausgewählt haben. Um all diese Werte — Region, und Schlüssel-ID — zu identifizieren AWS-Konto, sehen Sie sich den ARN Ihres KMS-Schlüssels an. Informationen, um die ARN des Schlüssels zu finden, finden Sie unter Schlüssel-ID und ARN suchen.

Ersetzen Sie auf ähnliche Weise *111122223333* durch das des AWS-Konto Kontos. GuardDuty Ersetzen Sie *Region2* durch die Region des Kontos. GuardDuty Ersetzen Sie *SourceDetectorID* durch die Melder-ID des GuardDuty Kontos für *Region2*.

Informationen zur Angabe `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

l. Wählen Sie Speichern.

2. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

3. Wählen Sie im Navigationsbereich Settings (Einstellungen).
4. Wählen Sie unter Exportoptionen für Erkenntnisse die Option Jetzt konfigurieren.
5. Wählen Sie Neuer Bucket. Geben Sie einen eindeutigen Namen für Ihren S3-Bucket ein.
6. (Optional) Sie können Ihre neuen Exporteinstellungen testen, indem Sie Beispiel-Erkenntnisse generieren. Wählen Sie im Navigationsbereich Settings (Einstellungen).
7. Wählen Sie unter dem Abschnitt Beispiel-Erkenntnisse die Option Beispiel-Erkenntnisse erstellen. Die neuen Ergebnisse der Stichprobe werden als Einträge im S3-Bucket angezeigt, der GuardDuty in bis zu fünf Minuten erstellt wurde.

Schritt 4: Richten Sie GuardDuty Suchwarnungen über SNS ein

GuardDuty ist in Amazon integriert EventBridge, wodurch Befunddaten zur Verarbeitung an andere Anwendungen und Dienste gesendet werden können. Mit EventBridge Hilfe von GuardDuty Ergebnissen können Sie automatische Antworten auf Ihre Ergebnisse einleiten, indem Sie Findereignisse mit Zielen wie AWS Lambda Funktionen, Amazon EC2 Systems Manager Manager-Automatisierung, Amazon Simple Notification Service (SNS) und mehr verknüpfen.

In diesem Beispiel erstellen Sie ein SNS-Thema, das das Ziel einer EventBridge Regel sein soll. Anschließend erstellen Sie EventBridge eine Regel, die Ergebnisdaten erfasst. GuardDuty Die resultierende Regel leitet die Erkenntnisdetails an eine E-Mail-Adresse weiter. Weitere Informationen dazu, wie Sie Erkenntnisse an Slack oder Amazon Chime senden und auch die Arten der Benachrichtigungen zu Erkenntnissen ändern können, finden Sie unter Einrichten eines Amazon-SNS-Themas und eines Endpunkts.

So erstellen Sie ein SNS-Thema für Ihre Benachrichtigungen zu Erkenntnissen

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie im Navigationsbereich Themen aus.
3. Wählen Sie Create Topic (Thema erstellen) aus.
4. Wählen Sie für Typ die Option Standard.
5. Geben Sie unter Name **`GuardDuty`** ein.
6. Wählen Sie Create Topic (Thema erstellen) aus. Die Themendetails für Ihr neues Thema werden geöffnet.
7. Wählen Sie im Abschnitt Subscriptions (Abonnements) die Option Create subscription (Abonnement erstellen) aus.

8. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus.
9. Geben Sie als Endpunkt die E-Mail-Adresse ein, an die Benachrichtigungen gesendet werden sollen.
10. Wählen Sie Create subscription (Abonnement erstellen) aus.

    Sie müssen Ihre E-Mail-Adresse bestätigen, nachdem Sie das Abonnement erstellt haben.
11. Um nach einer Abonnementnachricht zu suchen, gehen Sie zu Ihrem E-Mail-Posteingang und wählen Sie in der Abonnementnachricht die Option Abonnement bestätigen.

> **Note**
>
> Um den Status der E-Mail-Bestätigung zu überprüfen, rufen Sie die SNS-Konsole auf und wählen Sie Abonnements.

Um eine EventBridge Regel zu erstellen, um GuardDuty Ergebnisse zu erfassen und zu formatieren

1. Öffnen Sie die EventBridge Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Rules aus.
3. Wählen Sie Regel erstellen aus.
4. Geben Sie einen Namen und eine Beschreibung für die Regel ein.

   Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.
5. Bei Event bus (Ereignisbus) wählen Sie default (Standard) aus.
6. Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.
7. Wählen Sie Weiter aus.
8. Wählen Sie unter Event source (Ereignisquelle) AWS events (Ereignisse) aus.
9. Wählen Sie für Ereignismuster die Option Ereignismusterformular.
10. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.
11. Wählen Sie unter AWS -Service die Option GuardDuty aus.
12. Wählen Sie als Ereignistyp die Option GuardDutyFinding aus.
13. Wählen Sie Weiter aus.

14. Bei Target types (Zieltypen) wählen Sie AWS -Service aus.
15. Wählen Sie für Ziel auswählen das SNS-Thema und für Thema den Namen des SNS-Themas, das Sie zuvor erstellt haben.
16. Wählen Sie im Abschnitt Zusätzliche Einstellungen unter Zieleingabe konfigurieren die Option Eingabe-Transformer.

    Durch das Hinzufügen eines Eingangstransformators werden die gesendeten JSON-Suchdaten GuardDuty in eine für Menschen lesbare Nachricht formatiert.
17. Wählen Sie Configure input transformer (Eingabetransformator konfigurieren).
18. Fügen Sie im Abschnitt Ziel-Eingabe-Transformer für Eingabepfad den folgenden Code ein:

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_description": "$.detail.description"
}
```

19. Um die E-Mail zu formatieren, fügen Sie für Template den folgenden Code ein und achten Sie darauf, den roten Text durch die Werte zu ersetzen, die Ihrer Region entsprechen:

```
"You have a severity severity GuardDuty finding type Finding_Type in
 the Region_Name Region."
"Finding Description:"
"Finding_Description."
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=region#/findings?search=id%3DFinding_ID"
```

20. Wählen Sie Bestätigen aus.
21. Wählen Sie Weiter aus.
22. (Optional) Geben Sie ein oder mehrere Tags für die Regel ein. Weitere Informationen finden Sie unter EventBridge Amazon-Tags im EventBridge Amazon-Benutzerhandbuch.
23. Wählen Sie Weiter aus.
24. Überprüfen Sie die Details der Regel und wählen Sie dann Create rule (Regel erstellen) aus.

25. (Optional) Testen Sie Ihre neue Regel, indem Sie anhand des in Schritt 2 beschriebenen Prozesses Beispiel-Erkenntnisse generieren. Sie erhalten für jede generierte Beispiel-Erkenntnis eine E-Mail.

Nächste Schritte

Wenn Sie die Nutzung fortsetzen GuardDuty, werden Sie verstehen, welche Arten von Ergebnissen für Ihre Umgebung relevant sind. Wenn Sie eine neue Erkenntnis erhalten, können Sie Informationen, einschließlich Empfehlungen zur Problembehebung, zu dieser Erkenntnis finden, indem Sie in der Beschreibung der Erkenntnis im Bereich mit den Erkenntnisdetails die Option Weitere Informationen auswählen oder indem Sie unter nach dem Namen der Erkenntnis in Erkenntnistypen suchen.

Die folgenden Funktionen helfen Ihnen bei der Feinabstimmung, GuardDuty sodass die relevantesten Ergebnisse für Ihre AWS Umgebung bereitgestellt werden können:

- Um Ergebnisse auf einfache Weise nach bestimmten Kriterien wie Instanz-ID, Konto-ID, S3-Bucket-Name und mehr zu sortieren, können Sie darin Filter erstellen und speichern GuardDuty. Weitere Informationen finden Sie unter Filtern von Ergebnissen.
- Wenn Sie Erkenntnisse zu erwartetem Verhalten in Ihrer Umgebung erhalten, können Sie die Erkenntnisse anhand der Kriterien, die Sie mit Unterdrückungsregeln definieren, automatisch archivieren.
- Um zu verhindern, dass Ergebnisse anhand einer Teilmenge vertrauenswürdiger IPs generiert werden, oder um GuardDuty Monitor-IPs außerhalb des normalen Überwachungsbereichs zu platzieren, können Sie Listen vertrauenswürdiger IP-Adressen und Bedrohungen einrichten.

Konzepte und Terminologie

Wenn Sie mit Amazon beginnen GuardDuty, können Sie davon profitieren, mehr über die wichtigsten Konzepte zu erfahren.

Account

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

Sie können auch andere Konten einladen, Ihr AWS Konto zu aktivieren GuardDuty und mit diesem verknüpft zu werden GuardDuty. Wenn Ihre Einladungen akzeptiert werden, wird Ihr Konto als GuardDuty Administratorkonto festgelegt und die hinzugefügten Konten werden zu Ihren Mitgliedskonten. Sie können dann die GuardDuty Ergebnisse dieser Konten in ihrem Namen einsehen und verwalten.

Benutzer des Administratorkontos können die GuardDuty Ergebnisse für ihr eigenes Konto und alle ihre Mitgliedskonten konfigurieren GuardDuty , einsehen und verwalten. Sie können bis zu 10.000 Mitgliedskonten anlegen GuardDuty.

Benutzer von Mitgliedskonten können die GuardDuty Ergebnisse in ihrem Konto konfigurieren GuardDuty sowie einsehen und verwalten (entweder über die GuardDuty Verwaltungskonsole oder die GuardDuty API). Benutzer von Mitgliedskonten können keine Ergebnisse in den Konten anderer Mitglieder anzeigen oder verwalten.

Ein AWS Konto kann nicht gleichzeitig GuardDuty Administratorkonto und Mitgliedskonto sein. Ein Konto kann nur eine AWS -Mitgliedschaftseinladung annehmen. Das Annehmen einer Mitgliedschaftseinladung ist optional.

Weitere Informationen finden Sie unter Verwaltung mehrerer Konten bei Amazon GuardDuty.

Detektor

Alle GuardDuty Ergebnisse sind einem Detektor zugeordnet, bei dem es sich um ein Objekt handelt, das den GuardDuty Dienst repräsentiert. Bei dem Detektor handelt es sich um eine regionale Einheit, und für jedes Gerät, das in GuardDuty Betrieb ist, ist ein AWS-Region eigener Detektor erforderlich. Wenn Sie GuardDuty in einer Region aktivieren, wird in dieser Region ein neuer Melder mit einer eindeutigen 32 alphanumerischen detectorId generiert. Das Format einer Detektor-ID ist `12abc34d567e8fa901bc2d34e56789f0`.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

> **Note**
>
> In Umgebungen mit mehreren Konten werden alle Erkenntnisse für Mitgliedskonten zum Detektor des Administratorkontos weitergeleitet.

Einige GuardDuty Funktionen werden über den Detektor konfiguriert, z. B. die Konfiguration der Häufigkeit von Benachrichtigungen über CloudWatch Ereignisse und die Aktivierung oder Deaktivierung optionaler Datenquellen für GuardDuty die Verarbeitung.

Datenquelle

Der Ursprung oder Speicherort eines Datensatzes. Um unbefugte oder unerwartete Aktivitäten in Ihrer AWS Umgebung zu erkennen. GuardDuty analysiert und verarbeitet Daten aus AWS CloudTrail Ereignisprotokollen, AWS CloudTrail Verwaltungsereignissen, AWS CloudTrail Datenereignissen für S3, VPC-Flussprotokollen, DNS-Protokollen, EKS-Auditprotokollen, Überwachung der RDS-Anmeldeaktivitäten und EBS-Volumes. Weitere Informationen finden Sie unter Grundlegende Datenquellen.

Funktion

Ein für Ihren GuardDuty Schutzplan konfiguriertes Feature-Objekt hilft dabei, unbefugte oder unerwartete Aktivitäten in Ihrer AWS Umgebung zu erkennen. Jeder GuardDuty Schutzplan konfiguriert das entsprechende Featureobjekt zur Analyse und Verarbeitung von Daten. Zu den Feature-Objekten gehören EKS-Auditprotokolle, die Überwachung der RDS-Anmeldeaktivitäten und EBS-Volumes. Weitere Informationen finden Sie unter Funktionen Aktivierung in GuardDuty.

Erkenntnis

Ein von GuardDuty erkanntes potenzielles Sicherheitsrisiko. Weitere Informationen finden Sie unter Die GuardDuty Ergebnisse von Amazon verstehen.

Die Ergebnisse werden in der GuardDuty Konsole angezeigt und enthalten eine detaillierte Beschreibung des Sicherheitsproblems. Sie können Ihre generierten Ergebnisse auch abrufen, indem Sie die Operationen GetFindingsund die ListFindingsAPI aufrufen.

Sie können Ihre GuardDuty Ergebnisse auch über Amazon CloudWatch Events einsehen. GuardDuty sendet Ergebnisse CloudWatch über das HTTPS-Protokoll an Amazon. Weitere

Informationen finden Sie unter Erstellen von benutzerdefinierten Antworten auf GuardDuty Erkenntnisse mit Amazon CloudWatch Events.

Scan-Optionen

Wenn der GuardDuty Malware-Schutz aktiviert ist, können Sie angeben, welche Amazon EC2-Instances und Amazon Elastic Block Store (EBS) -Volumes gescannt oder übersprungen werden sollen. Mit diesem Feature können Sie die vorhandenen Tags, die Ihren EC2-Instances und Ihrem EBS-Volume zugeordnet sind, entweder zu einer Liste mit Einschluss-Tags oder einer Liste mit Ausschluss-Tags hinzufügen. Die Ressourcen, die mit den Tags verknüpft sind, die Sie zu einer Liste mit Einschlusstags hinzufügen, werden auf Malware gescannt, und die Ressourcen, die zu einer Ausschlusstag-Liste hinzugefügt wurden, werden nicht gescannt. Weitere Informationen finden Sie unter Scan-Optionen mit benutzerdefinierten Tags.

Snapshot-Beibehaltung

Wenn der GuardDuty Malware-Schutz aktiviert ist, können Sie die Snapshots Ihrer EBS-Volumes in Ihrem Konto behalten. AWS GuardDuty generiert die Replikat-EBS-Volumes auf der Grundlage der Snapshots Ihrer EBS-Volumes. Sie können die Snapshots Ihrer EBS-Volumes nur dann beibehalten, wenn der Scan von Malware Protection Malware in den EBS-Replikat-Volumes erkennt. Wenn in den EBS-Replikat-Volumes keine Schadsoftware erkannt wird, GuardDuty werden die Snapshots Ihrer EBS-Volumes unabhängig von der Aufbewahrungseinstellung für Snapshots automatisch gelöscht. Weitere Informationen finden Sie unter Snapshot-Beibehaltung.

Unterdrückungsregel

Unterdrückungsregeln ermöglichen die Einrichtung sehr spezifischer Kombinationen von Attributen, um Ergebnisse zu unterdrücken. Sie können beispielsweise über den GuardDuty Filter eine Regel definieren, um nur die Instances in einer bestimmten VPC, auf der ein bestimmtes AMI oder mit einem bestimmten EC2-Tag ausgeführt wird, automatisch zu archivieren`Recon:EC2/Portscan`. Diese Regel würde dazu führen, dass Port-Scan-Ergebnisse von den Instances automatisch archiviert werden, die die Kriterien erfüllen. Es ermöglicht jedoch weiterhin Warnmeldungen, wenn Instances GuardDuty entdeckt werden, die andere bösartige Aktivitäten wie das Mining von Kryptowährungen ausführen.

Die im GuardDuty Administratorkonto definierten Unterdrückungsregeln gelten für die Mitgliedskonten GuardDuty . GuardDuty Mitgliedskonten können die Unterdrückungsregeln nicht ändern.

Bei Unterdrückungsregeln werden GuardDuty trotzdem alle Ergebnisse generiert. Die Unterdrückungsregeln sorgen für eine Unterdrückung von Ergebnissen, während gleichzeitig ein vollständiger und unveränderlicher Verlauf aller Aktivitäten aufgezeichnet wird.

Gewöhnlich werden Unterdrückungsregeln verwendet, um Ergebnisse zu verbergen, die Sie als falsch positive Ergebnisse für Ihre Umgebung ermittelt haben, und um das Rauschen durch Ergebnisse mit niedrigem Wert zu reduzieren, sodass Sie sich auf größere Bedrohungen konzentrieren können. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Liste vertrauenswürdiger IPs

Eine Liste vertrauenswürdiger IP-Adressen für die hochsichere Kommunikation mit Ihrer AWS Umgebung. GuardDuty generiert keine Ergebnisse auf der Grundlage vertrauenswürdiger IP-Listen. Weitere Informationen finden Sie unter Arbeiten mit vertrauenswürdigen IP- und Bedrohungslisten.

Liste der bedrohlichen IP-Adressen

Eine Liste bekannter böswilliger IP-Adressen. Generiert nicht nur Ergebnisse aufgrund einer potenziell verdächtigen Aktivität, GuardDuty sondern generiert auch Ergebnisse auf der Grundlage dieser Bedrohungslisten. Weitere Informationen finden Sie unter Arbeiten mit vertrauenswürdigen IP- und Bedrohungslisten.

Funktionen Aktivierung in GuardDuty

Wenn Sie Amazon GuardDuty zum ersten Mal aktivieren oder darin einen Schutztyp aktivieren GuardDuty, GuardDuty beginnt die Verarbeitung des entsprechenden Schutzes Grundlegende Datenquellen in Ihrer AWS Umgebung. GuardDuty verwendet diese Datenquellen, um einen Strom von Ereignissen zu verarbeiten, z. B. VPC-Flussprotokolle, DNS-Protokolle sowie AWS CloudTrail Ereignis- und Verwaltungsprotokolle. Anschließend analysiert es diese Ereignisse, um potenzielle Sicherheitsbedrohungen zu identifizieren, und generiert Erkenntnisse in Ihrem Konto.

GuardDuty Kann neben Protokolldatenquellen auch zusätzliche Daten von anderen AWS Diensten in Ihrer AWS Umgebung verwenden, um potenzielle Sicherheitsbedrohungen zu überwachen und zu analysieren.

Feature-Aktivierung

Wenn Sie zusätzliche GuardDuty Schutzmaßnahmen hinzufügen, z. B. S3-Schutz, Runtime Monitoring oder EKS-Schutz, können Sie die GuardDuty Funktion entsprechend dem Schutztyp konfigurieren. In der Vergangenheit wurden GuardDuty Schutzmaßnahmen `dataSources` in den APIs aufgerufen. Nach März 2023 werden neue GuardDuty Schutztypen nun jedoch als `features` und nicht `dataSources` konfiguriert. GuardDuty unterstützt weiterhin die Konfiguration von Schutztypen, die vor März 2023 eingeführt wurden, wie `dataSources` über die API, aber neue Schutztypen sind nur als verfügbar`features`.

Wenn Sie GuardDuty Konfiguration und Schutztypen über die Konsole verwalten, sind Sie von dieser Änderung nicht direkt betroffen und müssen keine Maßnahmen ergreifen. Die Aktivierung von Funktionen wirkt sich auf das Verhalten der APIs aus, die zur Aktivierung aufgerufen werden, GuardDuty oder auf die darin enthaltenen Schutztypen. GuardDuty Weitere Informationen finden Sie unter GuardDuty API-Änderungen.

GuardDuty API-Änderungen im März 2023

Die GuardDuty APIs konfigurieren Schutzfunktionen, die nicht zur Liste der gehörenGrundlegende Datenquellen. Ein Feature-Objekt enthält Feature-Details, wie Feature-Namen und Status, und kann zusätzliche Konfigurationen für einige Feature enthalten. Diese Migration wirkt sich auf die folgenden APIs in der Amazon GuardDuty API-Referenz aus:

- CreateDetector

- GetDetector
- UpdateDetector
- GetMemberDetectors
- UpdateMemberDetectors
- DescribeOrganizationConfiguration
- UpdateOrganizationConfiguration
- GetRemainingFreeTrialDays
- GetUsageStatistics

Funktion-Aktivierung im Vergleich zu Datenquellen

In der Vergangenheit wurden alle GuardDuty Funktionen über ein `dataSources` Objekt in der API übergeben. Ab März 2023 GuardDuty bevorzugt `features` das Objekt anstelle des `dataSources` Objekts in der API. Alle früheren Datenquellen verfügen über entsprechende Feature, aber neuere Feature verfügen möglicherweise nicht über entsprechende Datenquellen.

Die folgende Liste zeigt den Vergleich zwischen einem `dataSources`-Objekt und einem `features`-Objekt, wenn es über eine API übergeben wird:

- Das `dataSources`-Objekt enthält Objekte für jeden Schutztyp und seinen Status. Das `features` Objekt ist eine Liste verfügbarer Funktionen, die jedem darin enthaltenen Schutztyp entsprechen GuardDuty.

  Ab März 2023 ist die Aktivierung von Funktionen die einzige Möglichkeit, neue GuardDuty Funktionen in Ihrer AWS Umgebung zu konfigurieren.
- Das `dataSources` Schema in der API-Anfrage oder -Antwort GuardDuty ist AWS-Region in allen verfügbaren Bereichen dasselbe. Möglicherweise sind nicht alle Feature von in jeder Region verfügbar. Daher können sich die Namen der verfügbaren Feature je nach Region unterscheiden.

Verstehen, wie die Aktivierung von Features funktioniert

Die GuardDuty APIs geben weiterhin ein `dataSources` Objekt zurück, sofern zutreffend, und sie geben auch ein `features` Objekt zurück, das dieselben Informationen in einem anderen Format enthält. GuardDuty Funktionen, die vor März 2023 eingeführt wurden, werden über `dataSources` Objekt und `features` Objekt verfügbar sein. GuardDuty Funktionen, die seit März 2023 eingeführt wurden, werden nur über das `features` Objekt verfügbar sein. Sie können in derselben API-

Anfrage keinen Detektor erstellen oder aktualisieren oder AWS Organizations beschreiben, indem Sie beide Objektnotationen `dataSources` und `features` verwenden. Um GuardDuty Schutztypen zu aktivieren, müssen Sie Ihre vorhandenen Datenquellen auf das `features` Objekt migrieren, indem Sie dieselben APIs verwenden, die jetzt auch das `features` Objekt enthalten.

> **Note**
>
> GuardDuty fügt nach dieser Änderung keine neue Datenquelle hinzu.

GuardDuty hat die Verwendung von Datenquellen eingestellt. Es unterstützt jedoch weiterhin die Grundlegende Datenquellen. Die GuardDuty bewährten Methoden empfehlen, die Aktivierung von Funktionen für alle Schutzarten zu verwenden, die bereits für Ihr Konto aktiviert sind. Die bewährten Methoden erfordern außerdem die Aktivierung von Features, wenn Sie einen neuen Schutztyp für Ihr Konto aktivieren.

Änderungen bei der Aktivierung von Features einbeziehen

- Wenn Sie GuardDuty Konfigurationen über APIs, SDKs oder AWS CloudFormation Vorlagen verwalten und potenzielle neue GuardDuty Funktionen aktivieren möchten, müssen Sie Ihren Code bzw. Ihre Vorlage ändern. Weitere Informationen finden Sie in der Amazon GuardDuty API-Referenz zu den aktualisierten APIs.
- Für GuardDuty Funktionen, die vor diesem Upgrade konfiguriert wurden, können Sie die APIs, SDKs oder die AWS CloudFormation Vorlage weiterhin verwenden. Wir empfehlen jedoch, zur Verwendung von `feature`-Objekt zu wechseln.

  Alle Datenquellen haben ein äquivalentes Feature-Objekt. Weitere Informationen finden Sie unter Zuordnung von `dataSources` zu `features`.
- Derzeit ist `additionalConfiguration` im `features`-Objekt nur für bestimmte Schutzarten verfügbar.
  - Für solche Schutztypen gilt: Wenn Ihre Funktion auf eingestellt `AdditionalConfiguration` `status` ist, die Konfiguration Ihrer Funktion `ENABLED` jedoch nicht aktiviert `status` ist`ENABLED`, GuardDuty werden in diesem Fall keine Maßnahmen ergriffen.
  - Die folgenden APIs sind davon betroffen:
    - UpdateDetector
    - UpdateMemberDetectors

- UpdateOrganizationConfiguration

Zuordnung von **`dataSources`** zu **`features`**

Die folgende Tabelle zeigt die Zuordnung der Schutztypen, `dataSources` und `features`.

GuardDuty Schutztyp	Name der Datenquelle *	Feature name
VPC Flow Logs	`flowLogs` (schreibgeschützt; kann nicht geändert werden)	`FLOW_LOGS` (schreibgeschützt; kann nicht geändert werden)
DNS-Protokolle	`dnsLogs` (schreibgeschützt; kann nicht geändert werden)	`DNS_LOGS` (schreibgeschützt; kann nicht geändert werden)
CloudTrail Ereignisse	`cloudLogs` (schreibgeschützt; kann nicht geändert werden)	`CLOUD_LOGS` (schreibgeschützt; kann nicht geändert werden)
S3	`s3Logs`	`S3_DATA_EVENTS`
EKS Audit Log Monitoring	`kubernetes.auditlogs`	`EKS_AUDIT_LOGS`
Malware Protection	`malwareProtection.scanEc2InstanceWithFindings.ebsVolumes`	`EBS_MALWARE_PROTECTION`

GuardDuty Schutztyp	Name der Datenquelle *	Feature name
RDS-Anmeldeereignisse	GuardDuty bietet nur Unterstützung für die Aktivierung von Funktionen für diese Schutztypen.	`RDS_LOGIN_EVENTS`
EKS-Laufzeit-Überwachung		`EKS_RUNTIME_MONITORING`
Überwachung der Laufzeit		`RUNTIME_MONITORING`

GuardDuty Sicherheitsagent für Amazon EKS-Cluster		`EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`
		
		`RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`

GuardDuty Sicherheitsagent für Amazon ECS-Fargate-Cluster		`RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT`

GuardDuty Schutztyp	Name der Datenquelle *	Feature name
GuardDuty Sicherheitsagent für Amazon EC2 EC2-Instances		`RUNTIME_MONITORING.additionalConfiguration.EC2_AGENT_MANAGEMENT`
Lambda Protection	`LAMBDA_NETWORK_LOGS`	

* GetUsageStatistics verwendet seine eigenen `dataSource`-Namen. Weitere Informationen finden Sie unter Schätzung der Kosten GuardDuty oder GetUsageStatistics.

Grundlegende Datenquellen

GuardDuty verwendet die grundlegenden Datenquellen, um die Kommunikation mit bekannten bösartigen Domänen und IP-Adressen zu erkennen und anomales Verhalten zu identifizieren. Bei der Übertragung von diesen Quellen zu GuardDuty werden alle Protokolldaten verschlüsselt. GuardDutyextrahiert verschiedene Felder aus diesen Protokollquellen für die Profilerstellung und die Erkennung von Anomalien und verwirft diese Protokolle anschließend.

In den folgenden Abschnitten wird beschrieben, wie die einzelnen unterstützten GuardDuty Datenquellen verwendet werden. Wenn Sie GuardDuty in Ihrem aktivieren AWS-Konto, beginnt GuardDuty automatisch die Überwachung dieser Protokollquellen.

Themen

AWS CloudTrail Ereignisprotokolle

AWS CloudTrail bietet Ihnen einen Verlauf der AWS API-Aufrufe für Ihr Konto, einschließlich API-Aufrufe, die mithilfe der AWS SDKs AWS Management Console, der Befehlszeilentools und bestimmter AWS Dienste getätigt wurden. CloudTrail hilft Ihnen auch dabei, zu ermitteln, welche Benutzer und Konten AWS APIs für Dienste aufgerufen haben CloudTrail, die Quell-IP-Adresse, von der aus die Aufrufe aufgerufen wurden, und den Zeitpunkt, zu dem die Aufrufe aufgerufen wurden. Weitere Informationen finden Sie unter Was ist AWS CloudTrail im AWS CloudTrail - Benutzerhandbuch.

GuardDuty überwacht auch Verwaltungsereignisse CloudTrail . Wenn Sie diese GuardDuty Option aktivieren, werden CloudTrail Verwaltungsereignisse direkt CloudTrail über einen unabhängigen und duplizierten Ereignisstrom verarbeitet und Ihre CloudTrail Ereignisprotokolle analysiert. Beim GuardDuty Zugriff auf die in aufgezeichneten Ereignisse fallen keine zusätzlichen Gebühren an. CloudTrail

GuardDuty verwaltet Ihre CloudTrail Ereignisse nicht und hat auch keine Auswirkungen auf Ihre bestehenden CloudTrail Konfigurationen. Ebenso haben Ihre CloudTrail Konfigurationen keinen

Einfluss darauf, wie GuardDuty die Ereignisprotokolle genutzt und verarbeitet werden. Verwenden Sie die CloudTrail Servicekonsole oder API, um den Zugriff auf Ihre CloudTrail Ereignisse und deren Aufbewahrung zu verwalten. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Wie GuardDuty geht man mit AWS CloudTrail globalen Ereignissen um

Bei den meisten AWS Diensten werden CloudTrail Ereignisse dort aufgezeichnet, AWS-Region wo sie erstellt wurden. Für globale Dienste wie AWS Identity and Access Management (IAM), AWS Security Token Service (AWS STS), Amazon Simple Storage Service (Amazon S3) CloudFront, Amazon und Amazon Route 53 (Route 53) werden Ereignisse nur in der Region generiert, in der sie auftreten, aber sie haben globale Bedeutung.

Wenn GuardDuty CloudTrail globale Serviceereignisse mit Sicherheitswert wie Netzwerkkonfigurationen oder Benutzerberechtigungen verarbeitet werden, repliziert es diese Ereignisse und verarbeitet sie in jeder Region, in der Sie sie aktiviert haben. GuardDuty Dieses Verhalten trägt dazu bei, Benutzer- und Rollenprofile in jeder Region zu GuardDuty verwalten, was für die Erkennung ungewöhnlicher Ereignisse von entscheidender Bedeutung ist.

Wir empfehlen dringend, dass Sie alle aktivieren GuardDuty AWS-Regionen , die für Sie aktiviert sind. AWS-Konto Auf diese Weise GuardDuty können Sie Erkenntnisse über unbefugte oder ungewöhnliche Aktivitäten gewinnen, auch in den Regionen, die Sie möglicherweise nicht aktiv nutzen.

AWS CloudTrail Management-Ereignisse

Verwaltungsereignisse werden auch als Ereignisse auf der Steuerebene bezeichnet. Diese Ereignisse bieten Einblick in Verwaltungsvorgänge, die mit Ressourcen in Ihrem AWS Konto ausgeführt werden.

Im Folgenden finden Sie Beispiele für CloudTrail Verwaltungsereignisse, die GuardDuty überwacht werden:

- Konfigurieren von Sicherheit (z. B. `AttachRolePolicy`-API-Vorgänge von IAM)
- Konfigurieren von Regeln für die Datenweiterleitung (z. B. `CreateSubnet`-API-Vorgänge von Amazon EC2)
- Einrichtung der Protokollierung (AWS CloudTrail `CreateTrail`API-Operationen)

VPC Flow Logs

Die VPC Flow Logs-Funktion von Amazon VPC erfasst Informationen über den IP-Verkehr zu und von Netzwerkschnittstellen, die mit den Amazon Elastic Compute Cloud (Amazon EC2) -Instances in Ihrer Umgebung verbunden sind. AWS

Wenn Sie es aktivieren GuardDuty, beginnt es sofort mit der Analyse Ihrer VPC-Flow-Logs von Amazon EC2 EC2-Instances in Ihrem Konto. Es nutzt VPC-Flow-Protokoll-Ereignisse direkt über das VPC-Flow-Protokoll-Feature durch einen unabhängigen und doppelt angelegten Flow-Protokollstrom. Dieser Prozess wirkt sich nicht auf ggf. vorhandene Flow-Protokollkonfigurationen aus.

GuardDuty Lambda-Schutz

Lambda Protection ist eine optionale Erweiterung für Amazon GuardDuty. Derzeit umfasst Lambda Network Activity Monitoring Amazon-VPC-Flow-Protokolle von allen Lambda-Funktionen für Ihr Konto, auch solche, die kein VPC-Netzwerk verwenden. Um Ihre Lambda-Funktion vor potenziellen Sicherheitsbedrohungen zu schützen, müssen Sie Lambda Protection in Ihrem GuardDuty Konto konfigurieren. Weitere Informationen finden Sie unter GuardDuty Lambda-Schutz.

GuardDuty Überwachung der Laufzeit

Wenn Sie den Security Agent (entweder manuell oder über GuardDuty) in EKS Runtime Monitoring oder Runtime Monitoring for EC2-Instances verwalten und derzeit auf einer Amazon EC2 EC2-Instance bereitgestellt GuardDuty ist und diese Gesammelte Laufzeit-Ereignistypen von dieser Instance empfängt, GuardDuty wird Ihnen die Analyse der VPC-Flow-Logs von dieser Amazon EC2 EC2-Instance nicht in Rechnung gestellt. AWS-Konto Dies trägt dazu bei, doppelte Nutzungskosten für das Konto GuardDuty zu vermeiden.

GuardDuty verwaltet Ihre Flow-Logs nicht und macht sie auch nicht in Ihrem Konto zugänglich. Damit Sie den Zugriff und die Aufbewahrung Ihrer Flow-Protokolle verwalten können, müssen Sie das Feature VPC-Flow-Protokolle konfigurieren.

DNS-Protokolle

Wenn Sie AWS DNS-Resolver für Ihre Amazon EC2 EC2-Instances verwenden (Standardeinstellung), GuardDuty können Sie über die internen AWS DNS-Resolver auf Ihre Anfrage- und Antwort-DNS-Protokolle zugreifen und diese verarbeiten. Wenn Sie einen anderen DNS-

Resolver wie OpenDNS oder GoogleDNS verwenden oder wenn Sie Ihre eigenen DNS-Resolver einrichten, GuardDuty können Sie nicht auf Daten aus dieser Datenquelle zugreifen und diese verarbeiten.

Wenn Sie diese Option aktivieren GuardDuty, werden Ihre DNS-Protokolle sofort anhand eines unabhängigen Datenstroms analysiert. Dieser Datenstrom ist von den Daten getrennt, die über das Feature Route-53-Resolver-Abfrageprotokollierung bereitgestellt werden. Die Konfiguration dieser Funktion hat keinen Einfluss auf die GuardDuty Analyse.

> **Note**
>
> GuardDuty unterstützt nicht die Überwachung von DNS-Protokollen für Amazon EC2 EC2-Instances, auf denen gestartet wurde, AWS Outposts da die Amazon Route 53 Resolver Abfrageprotokollierungsfunktion in dieser Umgebung nicht verfügbar ist.

EKS-Schutz bei Amazon GuardDuty

EKS Audit Log Monitoring hilft Ihnen dabei, potenziell verdächtige Aktivitäten in EKS-Clustern innerhalb von Amazon Elastic Kubernetes Service (Amazon EKS) zu erkennen. EKS Audit Log Monitoring verwendet EKS-Auditprotokolle, um chronologische Aktivitäten von Benutzern, Anwendungen, die die Kubernetes-API verwenden, und der Kontrollebene zu erfassen. Weitere Informationen finden Sie unter Überwachung des EKS-Auditprotokolls.

> **Note**
>
> EKS Runtime Monitoring wird als Teil von Runtime Monitoring verwaltet. Weitere Informationen finden Sie unter GuardDuty Überwachung der Laufzeit.

Funktionen in EKS Protection

Überwachung des EKS-Auditprotokolls

EKS-Auditprotokolle erfassen sequentielle Aktionen innerhalb Ihres Amazon EKS-Clusters, einschließlich Aktivitäten von Benutzern, Anwendungen, die die Kubernetes-API verwenden, und der Kontrollebene. Die Prüfungs-Protokollierung ist eine Komponente aller Kubernetes-Cluster.

Weitere Informationen finden Sie unter Prüfung in der Kubernetes-Dokumentation.

Amazon EKS ermöglicht die Erfassung von EKS-Auditprotokollen als Amazon CloudWatch Logs über die Protokollierungsfunktion der EKS-Kontrollebene. GuardDuty verwaltet die Protokollierung Ihrer Amazon EKS-Kontrollebene nicht und macht EKS-Auditprotokolle in Ihrem Konto nicht zugänglich, wenn Sie sie nicht für Amazon EKS aktiviert haben. Um den Zugriff auf und die Aufbewahrung Ihrer EKS-Auditprotokolle zu verwalten, müssen Sie die Protokollierungsfunktion der Amazon EKS-Kontrollebene konfigurieren. Weitere Informationen finden Sie unter Aktivieren und Deaktivieren von Protokollen auf Steuerebene im Amazon-EKS-Benutzerhandbuch.

Informationen zur Konfiguration von EKS Audit Log Monitoring finden Sie unter EKS Audit Log Monitoring.

EKS Audit Log Monitoring

EKS Audit Log Monitoring hilft Ihnen dabei, potenziell verdächtige Aktivitäten in Ihren EKS-Clustern innerhalb von Amazon Elastic Kubernetes Service zu erkennen. Wenn Sie EKS Audit Log Monitoring aktivieren, beginnt GuardDuty sofort mit der Überwachung Überwachung des EKS-Auditprotokolls Ihrer Amazon EKS-Cluster und deren Analyse auf potenziell bösartige und verdächtige Aktivitäten. Es verarbeitet Kubernetes-Audit-Log-Ereignisse direkt aus der Protokollierungsfunktion der Amazon EKS Control Plane über einen unabhängigen und duplizierten Stream von Audit-Logs. Dieser Prozess erfordert keine zusätzliche Einrichtung und hat auch keine Auswirkungen auf Ihre eventuell vorhandenen Konfigurationen der Amazon EKS-Protokollierung auf der Steuerebene.

Wenn Sie EKS Audit Log Monitoring deaktivieren, wird die Überwachung und Analyse der EKS-Auditprotokolle für Ihre Amazon EKS-Ressourcen GuardDuty sofort beendet.

EKS Audit Log Monitoring ist möglicherweise nicht überall verfügbar AWS-Regionen , wo GuardDuty es verfügbar ist. Weitere Informationen finden Sie unter Verfügbarkeit regionsspezifischer Feature.

Wie wirkt sich eine 30-tägige kostenlose Testphase auf Konten aus GuardDuty

- Wenn Sie EKS Audit Log Monitoring in EKS Protection GuardDuty zum ersten Mal aktivieren, ist es bereits in der kostenlosen 30-tägigen Testphase enthalten.
- Die vorhandenen GuardDuty Konten können EKS Audit Log Monitoring zum ersten Mal mit einer 30-tägigen kostenlosen Testphase aktivieren.

EKS Audit Log Monitoring für ein eigenständiges Konto konfigurieren

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Audit Log Monitoring für ein einzelnes Konto zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich EKS Protection.
3. Auf der Registerkarte Konfiguration können Sie den aktuellen Konfigurationsstatus von EKS Audit Log Monitoring einsehen. Wählen Sie im Abschnitt EKS Audit Log Monitoring die Option Aktivieren, um das Feature EKS Audit Log Monitoring zu aktivieren, oder Deaktivieren, um sie zu deaktivieren.
4. Wählen Sie Speichern.

API/CLI

- Führen Sie den updateDetectorAPI-Vorgang mit der regionalen Detektor-ID des delegierten GuardDuty Administratorkontos aus und übergeben Sie den `features` Objektnamen als `EKS_AUDIT_LOGS` und den Status als `ENABLED` oder`DISABLED`.

  Alternativ können Sie EKS Audit Log Monitoring auch aktivieren oder deaktivieren, indem Sie den AWS CLI Befehl a ausführen. Der folgende Beispielcode aktiviert GuardDuty EKS Audit Log Monitoring. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ - Konsole.

  ```
  aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  features [{"Name" : "EKS_AUDIT_LOGS", "Status" : "ENABLED"}]'
  ```

Konfiguration von EKS Audit Log Monitoring in Umgebungen mit mehreren Konten

In einer Umgebung mit mehreren Konten hat nur das delegierte GuardDuty Administratorkonto die Möglichkeit, die EKS-Funktion Audit Log Monitoring für die Mitgliedskonten in der jeweiligen Organisation zu aktivieren oder zu deaktivieren. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Dieses delegierte GuardDuty Administratorkonto kann wählen, ob EKS Audit Log Monitoring für alle neuen Konten automatisch aktiviert werden soll, wenn sie der Organisation beitreten. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten bei Amazon. GuardDuty

Konfiguration von EKS Audit Log Monitoring für ein delegiertes Administratorkonto GuardDuty

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Audit Log Monitoring für das delegierte GuardDuty Administratorkonto zu konfigurieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen des Verwaltungskontos verwenden.

2. Wählen Sie im Navigationsbereich EKS Protection aus.
3. Auf der Registerkarte Konfiguration können Sie den aktuellen Konfigurationsstatus von EKS Audit Log Monitoring im entsprechenden Abschnitt einsehen. Um die Konfiguration für das delegierte GuardDuty Administratorkonto zu aktualisieren, wählen Sie im Bereich EKS Audit Log Monitoring die Option Bearbeiten aus.
4. Führen Sie eine der folgenden Aktionen aus:

   Verwendung von Für alle Konten aktivieren

   - Wählen Sie Für alle Konten aktivieren. Dadurch wird der Schutzplan für alle aktiven GuardDuty Konten in Ihrer AWS Organisation aktiviert, einschließlich der neuen Konten, die der Organisation beitreten.
   - Wählen Sie Speichern.

   Verwendung von Konten manuell konfigurieren

   - Um den Schutzplan nur für das delegierte GuardDuty Administratorkonto zu aktivieren, wählen Sie Konten manuell konfigurieren.
   - Wählen Sie im Abschnitt für das delegierte GuardDuty Administratorkonto (dieses Konto) die Option Aktivieren aus.
   - Wählen Sie Speichern.

API/CLI

Führen Sie den API-Vorgang updateDetector aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen `name` als `EKS_AUDIT_LOGS` und `status` als `ENABLED` oder `DISABLED` übergeben.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

Sie können EKS Audit Log Monitoring aktivieren oder deaktivieren, indem Sie den folgenden AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie die gültige *`Melder-ID`* des delegierten GuardDuty Administratorkontos verwenden.

> **Note**
>
> Der folgende Beispielcode aktiviert EKS Audit Log Monitoring. *Achten Sie darauf, 12abc34d567e8fa901bc2d34e56789f0 durch die des delegierten Administratorkontos und 555555555555 durch die des delegierten Administratorkontos zu ersetzen. detector-id GuardDuty* AWS-Konto GuardDuty

Informationen `detectorId` zu den Einstellungen für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 555555555555 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

Um EKS Audit Log Monitoring zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Automatische Aktivierung von EKS Audit Log Monitoring für alle Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Audit Log Monitoring für alle vorhandenen aktiven Mitgliedskonten zu aktivieren.

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.

2. Führen Sie eine der folgenden Aktionen aus:

   Verwenden der Seite EKS Protection

   1. Wählen Sie im Navigationsbereich EKS Protection.
   2. Auf der Registerkarte Konfiguration können Sie den aktuellen Status von EKS Audit Log Monitoring für aktive Mitgliedskonten in Ihrer Organisation einsehen.

Um die Konfiguration von EKS Audit Log Monitoring zu aktualisieren, wählen Sie Bearbeiten.

3. Wählen Sie Für alle Konten aktivieren. Diese Aktion aktiviert EKS Audit Log Monitoring automatisch sowohl für die vorhandenen als auch für die neuen Konten in der Organisation.
4. Wählen Sie Speichern.

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Verwenden der Seite Konten

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren und anschließend Konten auf Einladung hinzufügen.
3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter EKS Audit Log Monitoring die Option Für alle Konten aktivieren.
4. Wählen Sie Speichern.

Wenn Sie die Option Für alle Konten aktivieren nicht verwenden können und die Konfiguration von EKS Audit Log Monitoring für bestimmte Konten in Ihrer Organisation anpassen möchten, finden Sie weitere Informationen unter Aktivieren oder deaktivieren Sie EKS Audit Log Monitoring selektiv für Mitgliedskonten.

API/CLI

- Um die EKS-Laufzeit-Überwachung selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen *`Detektor-ID`* aus.
- Das folgende Beispiel zeigt, wie Sie EKS Audit Log Monitoring für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
```

> **Note**
>
> Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivierung von EKS Audit Log Monitoring für alle vorhandenen aktiven Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Audit Log Monitoring für alle vorhandenen aktiven Mitgliedskonten zu aktivieren.

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldeinformationen für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich EKS Protection.
3. Auf der EKS-Schutzseite können Sie den aktuellen Status der Konfiguration des GuardDuty-initiierten Malware-Scans einsehen. Wählen Sie im Abschnitt Aktive Mitgliedskonten die Option Aktionen.
4. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
5. Wählen Sie Speichern.

API/CLI

- Um die EKS-Laufzeit-Überwachung selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen *`Detektor-ID`* aus.
- Das folgende Beispiel zeigt, wie Sie EKS Audit Log Monitoring für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivieren Sie EKS Audit Log Monitoring automatisch für neue Mitgliedskonten

Die neu hinzugefügten Mitgliedskonten müssen aktiviert werden, GuardDuty bevor die Konfiguration des GuardDuty -initiierten Malware-Scans ausgewählt werden kann. Die auf Einladung verwalteten Mitgliedskonten können den GuardDuty -initiierten Malware-Scan für ihre Konten manuell konfigurieren. Weitere Informationen finden Sie unter Step 3 - Accept an invitation.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Audit Log Monitoring für neue Konten zu aktivieren, die Ihrer Organisation beitreten.

Console

Das delegierte GuardDuty Administratorkonto kann EKS Audit Log Monitoring für neue Mitgliedskonten in einer Organisation entweder über die Seite EKS Audit Log Monitoring oder Konten aktivieren.

So aktivieren Sie EKS Audit Log Monitoring automatisch für neue Mitgliedskonten

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.

2. Führen Sie eine der folgenden Aktionen aus:

   - Verwenden der Seite EKS Protection:

     1. Wählen Sie im Navigationsbereich EKS Protection.
     2. Wählen Sie auf der Seite EKS Protection im Bereich EKS Audit Log Monitoring Bearbeiten.
     3. Wählen Sie Konten manuell konfigurieren.
     4. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Dieser Schritt stellt sicher, dass EKS Audit Log Monitoring bei jedem Beitritt eines neuen Kontos zu Ihrer Organisation automatisch für das Konto aktiviert wird. Nur das delegierte GuardDuty Administratorkonto der Organisation kann diese Konfiguration ändern.
     5. Wählen Sie Speichern.

   - Verwenden der Seite Konten:

     1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
     2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren.
     3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter EKS Audit Log Monitoring die Option Für neue Konten aktivieren.
     4. Wählen Sie Speichern.

API/CLI

- Um EKS Audit Log Monitoring selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den API-Vorgang UpdateOrganizationConfiguration mit Ihrer eigenen *`Detektor-ID`* aus.
- Das folgende Beispiel zeigt, wie Sie EKS Audit Log Monitoring für die neuen Mitglieder aktivieren können, die Ihrer Organisation beitreten. Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "EKS_AUDIT_LOGS", "AutoEnable": "NEW"}]'
```

Aktivieren oder deaktivieren Sie EKS Audit Log Monitoring selektiv für Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Audit Log Monitoring für alle vorhandenen aktiven Mitgliedskonten zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.

   Prüfen Sie auf der Seite Konten in der Spalte EKS Audit Log Monitoring den Status Ihres Mitgliedskontos.
3. So aktivieren oder deaktivieren Sie EKS Audit Log Monitoring

   Wählen Sie ein Konto aus, das Sie für EKS Audit Log Monitoring konfigurieren möchten. Sie können mehrere Konten gleichzeitig auswählen. Wählen Sie im Dropdown-Menü Schutzpläne bearbeiten die Option EKS Audit Log Monitoring und dann die entsprechende Option aus.

API/CLI

Um die EKS-Laufzeit-Überwachung selektiv für Ihre Mitgliedskonten zu aktivieren oder zu deaktivieren, führen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen *Detektor-ID* aus.

Das folgende Beispiel zeigt, wie Sie EKS Audit Log Monitoring für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`. Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 111122223333 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

Lambda-Schutz bei Amazon GuardDuty

Lambda Protection hilft Ihnen dabei, potenzielle Sicherheitsbedrohungen zu identifizieren, wenn eine AWS Lambda-Funktion in Ihrer AWS -Umgebung aufgerufen wird. Wenn Sie Lambda Protection aktivieren, GuardDuty beginnt die Überwachung VPC Flow Logs von Lambda-Netzwerkaktivitätsprotokollen, beginnend mit allen Lambda-Funktionen für Account, einschließlich der Protokolle, die kein VPC-Netzwerk verwenden, und die generiert werden, wenn die Lambda-Funktion aufgerufen wird. Wenn verdächtiger Netzwerkverkehr GuardDuty identifiziert wird, der auf das Vorhandensein eines potenziell schädlichen Codes in Ihrer Lambda-Funktion hinweist, GuardDuty wird ein Befund generiert.

> **Note**
>
> Lambda Network Activity Monitoring beinhaltet keine Protokolle für Lambda@Edge-Funktionen.

Sie können Lambda Protection für jedes Konto oder für jedes verfügbare AWS-Regionen Konto jederzeit konfigurieren. Standardmäßig kann ein vorhandenes GuardDuty Konto Lambda Protection mit einer 30-tägigen Testphase aktivieren. Für ein neues GuardDuty Konto ist Lambda Protection bereits aktiviert und in der 30-tägigen Testphase enthalten. Weitere Informationen zu Nutzungsstatistiken finden Sie unter Einschätzen der Kosten.

GuardDuty überwacht Netzwerkaktivitätsprotokolle, die durch den Aufruf der Lambda-Funktionen generiert wurden. Derzeit umfasst Lambda Network Activity Monitoring Amazon-VPC-Flow-Protokolle von allen Lambda-Funktionen für Ihr Konto, einschließlich der Protokolle, die kein VPC-Netzwerk verwenden und sich ändern können, einschließlich der Erweiterung auf andere Netzwerkaktivitäten wie DNS-Abfragedaten, die durch das Aufrufen der Lambda-Funktionen generiert werden. Die Ausweitung auf andere Formen der Überwachung der Netzwerkaktivität wird das Datenvolumen erhöhen, das für Lambda Protection verarbeitet GuardDuty wird. Dies wird sich direkt auf die Nutzungskosten von Lambda Protection auswirken. Wenn GuardDuty mit der Überwachung eines zusätzlichen Netzwerkaktivitätsprotokolls begonnen wird, erhalten die Konten, die Lambda Protection aktiviert haben, mindestens 30 Tage vor der Veröffentlichung eine Benachrichtigung.

Feature in Lambda Protection

Lambda Network Activity Monitoring

Wenn Sie Lambda Protection aktivieren, GuardDuty überwacht Lambda-Netzwerkaktivitätsprotokolle, die generiert werden, wenn eine Ihrem Konto zugeordnete Lambda-Funktion aufgerufen wird. Auf diese Weise können Sie potenzielle Sicherheitsbedrohungen für die Lambda-Funktion erkennen. GuardDuty überwacht VPC-Flussprotokolle all Ihrer Lambda-Funktionen, einschließlich derer, die kein VPC-Netzwerk verwenden. Für Lambda-Funktionen, die für die Verwendung von VPC-Netzwerken konfiguriert sind, müssen Sie keine VPC-Flussprotokolle für die von Lambda für erstellten Elastic Network Interfaces (ENI) aktivieren. GuardDuty GuardDuty berechnet nur die Menge an Lambda-Netzwerkaktivitätsprotokollen, die verarbeitet wurden (in GB), um ein Ergebnis zu generieren. GuardDuty optimiert die Kosten durch die Anwendung intelligenter Filter und die Analyse einer Teilmenge der Lambda-Netzwerkaktivitätsprotokolle, die für die Bedrohungserkennung relevant sind. Preisinformationen finden Sie unter GuardDuty Amazon-Preise.

GuardDuty verwaltet Ihre Lambda-Netzwerkaktivitätsprotokolle (einschließlich VPC- und Nicht-VPC-Flow-Logs) nicht und macht sie auch nicht in Ihrem Konto zugänglich.

Konfigurieren von Lambda Protection

Lambda Protection für ein einzelnes Konto konfigurieren

Für Konten, die mit verknüpft sind AWS Organizations, können Sie diesen Vorgang mithilfe von GuardDuty Konsolen- oder API-Anweisungen automatisieren, wie im nächsten Abschnitt beschrieben.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Protection für ein einzelnes Konto zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Lambda Protection.
3. Auf der Lambda-Protection-Seite wird der aktuelle Status Ihres Kontos angezeigt. Sie können das Feature jederzeit aktivieren oder deaktivieren, indem Sie Aktivieren oder Deaktivieren auswählen.
4. Wählen Sie Speichern.

API/CLI

Führen Sie den API-Vorgang updateDetector aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen `name` als `LAMBDA_NETWORK_LOGS` und `status` als `ENABLED` oder `DISABLED` übergeben.

Sie können Lambda Network Activity Monitoring auch aktivieren oder deaktivieren, indem Sie den folgenden AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie Ihre eigene gültige *Detektor-ID* verwenden.

> **Note**
>
> Der folgende Beispielcode aktiviert Lambda Network Activity Monitoring. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "LAMBDA_NETWORK_LOGS", "Status" : "ENABLED"}]'
```

Lambda Protection in Umgebungen mit mehreren Konten konfigurieren

In einer Umgebung mit mehreren Konten hat nur das delegierte GuardDuty Administratorkonto die Möglichkeit, Lambda Protection für die Mitgliedskonten in seiner Organisation zu aktivieren oder zu deaktivieren. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet Mitgliedskonten mithilfe von AWS Organizations. Das delegierte GuardDuty Administratorkonto kann festlegen, dass Lambda Network Activity Monitoring für alle neuen Konten automatisch aktiviert wird, sobald sie der Organisation beitreten. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten bei Amazon GuardDuty.

Lambda-Schutz für ein delegiertes Administratorkonto GuardDuty konfigurieren

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Network Activity Monitoring für das delegierte GuardDuty Administratorkonto zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen des Verwaltungskontos verwenden.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Lambda Protection.
3. Wählen Sie auf der Seite Lambda Protection die Option Bearbeiten.
4. Führen Sie eine der folgenden Aktionen aus:

   Verwendung von Für alle Konten aktivieren

   - Wählen Sie Für alle Konten aktivieren. Dadurch wird der Schutzplan für alle aktiven GuardDuty Konten in Ihrer AWS Organisation aktiviert, einschließlich der neuen Konten, die der Organisation beitreten.
   - Wählen Sie Speichern.

   Verwendung von Konten manuell konfigurieren

   - Um den Schutzplan nur für das delegierte GuardDuty Administratorkonto zu aktivieren, wählen Sie Konten manuell konfigurieren.
   - Wählen Sie im Abschnitt für das delegierte GuardDuty Administratorkonto (dieses Konto) die Option Aktivieren aus.
   - Wählen Sie Speichern.

API/CLI

Führen Sie den API-Vorgang updateDetector aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen `name` als `LAMBDA_NETWORK_LOGS` und `status` als `ENABLED` oder `DISABLED` übergeben.

Sie können Lambda Network Activity Monitoring aktivieren oder deaktivieren, indem Sie den folgenden AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie die gültige *`Detektor-ID`* des delegierten GuardDuty Administratorkontos verwenden.

> **Note**
>
> Der folgende Beispielcode aktiviert Lambda Network Activity Monitoring. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Die `detectorId` für Ihr Konto und Ihre aktuelle Region gültige Adresse finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 555555555555 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status":
 "ENABLED"}]'
```

Automatische Aktivierung von Lambda Network Activity Monitoring für alle Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Network Activity Monitoring Feature für alle Mitgliedskonten zu aktivieren. Dazu gehören der delegierte Administrator, bestehende Mitgliedskonten und die neuen Konten, die der Organisation beitreten.

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Führen Sie eine der folgenden Aktionen aus:

   Die Seite Lambda Protection verwenden

   1. Wählen Sie im Navigationsbereich Lambda Protection aus.
   2. Wählen Sie Für alle Konten aktivieren. Diese Aktion aktiviert automatisch Lambda Network Activity Monitoring sowohl für bestehende als auch für neue Konten in der Organisation.
   3. Wählen Sie Speichern.

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Verwenden der Seite Konten

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren und anschließend Konten auf Einladung hinzufügen.
3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter Lambda Network Activity Monitoring die Option Für alle Konten aktivieren.

   > **Note**
   >
   > Standardmäßig aktiviert diese Aktion automatisch die Option Automatisch GuardDuty für neue Mitgliedskonten aktivieren.

4. Wählen Sie Speichern.

Falls Sie die Option Für alle Konten aktivieren nicht verwenden können, finden Sie weitere Informationen unter Selektives Aktivieren oder Deaktivieren von Lambda Network Activity Monitoring für Mitgliedskonten.

API/CLI

- Um Lambda Network Activity Monitoring selektiv für ausgewählte neuen Konten zu aktivieren oder zu deaktivieren, rufen Sie den updateMemberDetectors-API-Vorgang mit Ihrer eigenen *`Detektor-ID`* auf.
- Das folgende Beispiel zeigt, wie Sie Lambda Network Activity Monitoring für ein einzelnes Mitgliedskonto aktivieren können. Um ein Mitgliedskonto zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivierung von Lambda Network Activity Monitoring für alle vorhandenen aktiven Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Network Activity Monitoring für alle vorhandenen aktiven Mitgliedskonten in der Organisation zu aktivieren.

Console

So konfigurieren Sie Lambda Network Activity Monitoring für alle vorhandenen aktiven Mitgliedskonten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldeinformationen für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich Lambda Protection.
3. Auf der Seite Lambda Protection können Sie den aktuellen Status der Konfiguration anzeigen. Wählen Sie im Abschnitt Aktive Mitgliedskonten die Option Aktionen.
4. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
5. Wählen Sie Bestätigen aus.

API/CLI

- Um Lambda Network Activity Monitoring selektiv für ausgewählte neuen Konten zu aktivieren oder zu deaktivieren, rufen Sie den updateMemberDetectors-API-Vorgang mit Ihrer eigenen *`Detektor-ID`* auf.
- Das folgende Beispiel zeigt, wie Sie Lambda Network Activity Monitoring für ein einzelnes Mitgliedskonto aktivieren können. Um ein Mitgliedskonto zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
  ```

  Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.
- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Automatische Aktivierung von Lambda Network Activity Monitoring für neue Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Network Activity Monitoring für neue Konten, die Ihrer Organisation beitreten, zu aktivieren.

Console

Das delegierte GuardDuty Administratorkonto kann Lambda Network Activity Monitoring für neue Mitgliedskonten in einer Organisation entweder über die Seite Lambda-Schutz oder Konten aktivieren.

Wie Sie die automatische Aktivierung von Lambda Network Activity Monitoring für neue Mitgliedskonten einrichten

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.

2. Führen Sie eine der folgenden Aktionen aus:

   - Verwenden der Seite Lambda Protection:

     1. Wählen Sie im Navigationsbereich Lambda Protection.
     2. Wählen Sie auf der Seite Lambda Protection die Option Bearbeiten.
     3. Wählen Sie Konten manuell konfigurieren.
     4. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Dieser Schritt stellt sicher, dass Lambda Protection automatisch für das Konto aktiviert wird, wann immer ein neues Konto Ihrer Organisation beitritt. Nur das delegierte GuardDuty Administratorkonto der Organisation kann diese Konfiguration ändern.
     5. Wählen Sie Speichern.

   - Verwenden der Seite Konten:

     1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
     2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren.
     3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter Lambda Network Activity Monitoring die Option Für neue Konten aktivieren.
     4. Wählen Sie Speichern.

API/CLI

- Um Lambda Network Activity Monitoring für ausgewählte neuen Konten zu aktivieren, rufen Sie den UpdateOrganizationConfiguration-API-Vorgang mit Ihrer eigenen *`Detektor-ID`* auf.
- Das folgende Beispiel zeigt, wie Sie Lambda Network Activity Monitoring für ein einzelnes Mitgliedskonto aktivieren können. Informationen zur Deaktivierung finden Sie unter Selektives Aktivieren oder Deaktivieren von Lambda Network Activity Monitoring für Mitgliedskonten. Wenn Sie es nicht für alle neuen Konten aktivieren möchten, die der Organisation beitreten, legen Sie die Einstellung `AutoEnable` auf `NONE` fest.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "AutoEnable": "NEW"}]'
```

Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Selektives Aktivieren oder Deaktivieren von Lambda Network Activity Monitoring für Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Network Activity Monitoring für ausgewählte Mitgliedskonten zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Klicken Sie im Navigationsbereich unter Settings auf Accounts.

   Sehen Sie sich auf der Seite Konten die Spalte Lambda Network Activity Monitoring an. Sie gibt an, ob Lambda Network Activity Monitoring aktiviert ist oder nicht.
3. Wählen Sie das Konto aus, für das Sie Lambda Protection konfigurieren möchten. Sie können mehrere Konten gleichzeitig auswählen.
4. Wählen Sie im Dropdownmenü Schutzpläne bearbeiten die Option Lambda Network Activity Monitoring und wählen Sie dann eine entsprechende Aktion aus.

API/CLI

Rufen Sie die updateMemberDetectors-API mit Ihrer eigenen Detektor-ID auf.

Das folgende Beispiel zeigt, wie Sie Lambda Network Activity Monitoring für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status":
 "ENABLED"}]'
```

Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Malware-Schutz bei Amazon GuardDuty

Malware Protection hilft Ihnen, das potenzielle Vorhandensein von Malware zu erkennen, indem es die Amazon Elastic Block Store (Amazon EBS)-Volumes scannt, die an die Amazon Elastic Compute Cloud (Amazon EC2)-Instances und Container-Workloads angefügt sind. Malware Protection bietet Scan-Optionen, mit denen Sie entscheiden können, ob Sie bestimmte Amazon-EC2-Instances und Container-Workloads beim Scannen ein- oder ausschließen möchten. Es bietet auch die Möglichkeit, die Snapshots der Amazon EBS-Volumes, die an die Amazon EC2 EC2-Instances oder Container-Workloads angehängt sind, in Ihren Konten aufzubewahren. GuardDuty Die Snapshots werden nur aufbewahrt, wenn Malware gefunden wird und die Erkenntnisse von Malware Protection generiert werden.

Malware Protection bietet zwei Arten von Scans zur Erkennung potenziell bösartiger Aktivitäten in Ihren Amazon EC2 EC2-Instances und Container-Workloads: den GuardDuty initiierten Malware-Scan und den On-Demand-Malware-Scan. Die folgende Tabelle zeigt den Vergleich zwischen den beiden Scan-Typen.

Faktor	GuardDuty-initiierter Malware-Scan	Malware-Scan auf Abruf
Wie der Scan aufgerufen wird	Sobald Sie den GuardDuty -initiierten Malware-Scan aktiviert haben, GuardDuty wird jedes Mal, wenn ein Ergebnis generiert wird, das auf das potenzielle Vorhanden sein von Malware in einer Amazon EC2 EC2-Insta nce oder einem Container-Workload hinweist, GuardDuty automatisch ein agentenlo ser Malware-Scan auf den Amazon EBS-Volumes initiiert, die an Ihre potenziell betroffen e Ressource angehängt sind. Weitere Informationen finden	Sie können einen Malware-S can auf Abruf einleiten, indem Sie den Amazon-Ressourcenn amen (ARN) angeben, der mit Ihrer Amazon-EC2-Instanc e oder Ihrem Container-Workload verknüpft ist. Sie können einen On-Demand-Malware-Scan starten, auch wenn für Ihre Ressource kein GuardDuty Ergebnis generiert wurde. Weitere Informationen finden Sie unter Malware-Scan auf Abruf.

Faktor	GuardDuty-initiierter Malware-Scan	Malware-Scan auf Abruf
	Sie unter GuardDuty-initiierter Malware-Scan.	
Konfiguration erforderlich	Um den GuardDuty -initiierten Malware-Scan verwenden zu können, müssen Sie ihn für Ihr Konto aktivieren. Weitere Informationen finden Sie unter Konfiguration des GuardDuty -initiierten Malware-Scans.	Ihr Konto muss GuardDuty aktiviert sein. Um den On-Demand-Malware-Scan zu verwenden, ist keine Konfiguration auf Funktionsebene erforderlich.
Wartezeit zum Initiieren eines neuen Scanvorgangs	Immer wenn ein Malware-Scan GuardDuty generiert wirdErgebnisse, die einen GuardDuty -initiierten Malware-Scan auslösen, wird nur einmal alle 24 Stunden automatisch ein Malware-Scan gestartet.	Sie können einen On-Demand -Malware-Scan für dieselbe Ressource jederzeit nach dem Start des vorherigen Scans starten.
Verfügbarkeit der 30-tägigen kostenlosen Testphase	Wenn Sie den GuardDuty -initiierten Malware-Scan in Ihrem Konto zum ersten Mal aktivieren, können Sie eine 30-tägige kostenlose Testphase nutzen*.	Es gibt keine kostenlose Testzeit* mit On-Demand -Malware-Scan für neue oder bestehende GuardDuty Konten.

Faktor	GuardDuty-initiierter Malware-Scan	Malware-Scan auf Abruf
Scan-Optionen	Nachdem Sie den von Ihnen GuardDuty initiierten Malware-Scan konfiguriert haben, hilft Ihnen der Malware-Schutz auch dabei, auszuwählen, welche Ressourcen gescannt oder übersprungen werden sollen. Malware Protection initiiert keinen automatischen Scan der Ressourcen, die Sie vom Scan ausschließen möchten.	Der Malware-Scan auf Abruf unterstützt ein globales Tag —`GuardDutyExcluded` . Scan-Optionen mit benutzerdefinierten Tagsgilt nicht für den On-Demand-Malware-Scan, da Sie den Ressourcen-ARN manuell angeben.

*Es fallen Nutzungskosten für die Erstellung von EBS-Volume-Snapshots und die Aufbewahrung von Snapshots an. Weitere Informationen zur Konfiguration Ihres Kontos für die Aufbewahrung von Snapshots finden Sie unterSnapshot-Beibehaltung.

Der Malware-Schutz ist eine optionale Erweiterung von und wurde so konzipiert, dass er die Leistung Ihrer Ressourcen nicht beeinträchtigt. GuardDuty Informationen zur Funktionsweise von GuardDuty Malware Protection finden Sie unterFeature in Malware Protection. Informationen zur Verfügbarkeit von Malware Protection in verschiedenen AWS-Regionen Ländern finden Sie unterRegionen und Endpunkte.

> **Note**
>
> GuardDuty Malware Protection unterstützt Fargate weder mit Amazon EKS noch mit Amazon ECS.

Feature in Malware Protection

Elastic Block Storage (EBS)-Volume

In diesem Abschnitt wird erklärt, wie Malware Protection, einschließlich GuardDuty initiierter Malware-Scans und On-Demand-Malware-Scans, die Amazon EBS-Volumes scannt, die Ihren Amazon EC2 EC2-Instances und Container-Workloads zugeordnet sind. Berücksichtigen Sie die folgenden Anpassungen, bevor Sie fortfahren:

- Scan-Optionen – Malware Protection bietet die Möglichkeit, Tags anzugeben, um Amazon-EC2-Instances und Amazon-EBS-Volumes in den Scanvorgang entweder ein- oder auszuschließen. Nur der GuardDuty -initiierte Malware-Scan unterstützt Scanoptionen mit benutzerdefinierten Tags. Sowohl der GuardDuty -initiierte Malware-Scan als auch der On-Demand-Malware-Scan unterstützen das globale Tag. `GuardDutyExcluded` Weitere Informationen finden Sie unter Scan-Optionen mit benutzerdefinierten Tags.
- Aufbewahrung von Snapshots — Malware Protection bietet eine Option, um die Snapshots Ihrer Amazon EBS-Volumes in Ihrem Konto aufzubewahren. AWS Diese Option ist standardmäßig ausgeschaltet. Sie können sich für die Aufbewahrung von Snapshots sowohl für GuardDuty initiierte als auch für On-Demand-Malware-Scans entscheiden. Weitere Informationen finden Sie unter Snapshot-Beibehaltung.

Wenn ein Ergebnis GuardDuty generiert wird, das auf das potenzielle Vorhandensein von Malware in einer Amazon EC2 EC2-Instance oder einem Container-Workload hinweist, und Sie den GuardDuty initiierten Scantyp in Malware Protection aktiviert haben, kann ein GuardDuty -initiierter Malware-Scan auf der Grundlage Ihrer Scanoptionen aufgerufen werden.

Um einen Malware-Scan auf Abruf auf den Amazon-EBS-Volumes zu initiieren, die mit einer Amazon-EC2-Instance verknüpft sind, geben Sie den Amazon-Ressourcennamen (ARN) der Amazon-EC2-Instance an.

Als Reaktion auf einen On-Demand-Malware-Scan oder einen automatisch aufgerufenen GuardDuty -initiierten Malware-Scan GuardDuty erstellt es Snapshots der relevanten EBS-Volumes, die an die potenziell betroffene Ressource angehängt sind, und gibt sie an die weiter. GuardDuty Dienstkonto GuardDuty Erstellt aus diesen Snapshots ein verschlüsseltes EBS-Replikat-Volume im Dienstkonto.

GuardDuty Löscht nach Abschluss des Scans die verschlüsselten EBS-Replikat-Volumes und die Snapshots Ihrer EBS-Volumes. Wenn Malware gefunden wird und Sie die Einstellung zur

Aufbewahrung von Snapshots aktiviert haben, werden die Snapshots Ihrer EBS-Volumes nicht gelöscht, sondern automatisch in Ihrem Konto gespeichert. AWS Wenn keine Malware gefunden wird, werden die Snapshots Ihrer EBS-Volumes nicht aufbewahrt, unabhängig von der Einstellung zur Aufbewahrung von Snapshots. Standardmäßig ist die Aufbewahrungseinstellung für Snapshots deaktiviert. Informationen zu den Kosten von Snapshots und deren Aufbewahrung finden Sie unter Amazon-EBS-Preise.

GuardDuty speichert jedes replizierte EBS-Volume im Servicekonto für bis zu 55 Stunden. Im Falle eines Dienstausfalls oder eines Fehlers bei einem EBS-Replikat-Volume und dessen Malware-Scan GuardDuty wird ein solches EBS-Volume nicht länger als sieben Tage aufbewahrt. Die verlängerte Aufbewahrungsfrist für das Volume dient der Suche und Behebung des Ausfalls oder Fehlers. GuardDuty Der Malware-Schutz löscht die replizierten EBS-Volumes aus dem Dienstkonto, nachdem der Ausfall oder Fehler behoben wurde oder wenn die erweiterte Aufbewahrungsfrist abgelaufen ist.

Unterstützte Amazon EBS-Volumes für Malware-Scans

In allen Ländern, in AWS-Regionen denen die Malware-Schutzfunktion GuardDuty unterstützt wird, können Sie die unverschlüsselten oder verschlüsselten Amazon EBS-Volumes scannen. Sie können Amazon EBS-Volumes verwenden, die entweder mit einem Von AWS verwalteter Schlüsseloder mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind. Derzeit AWS-Regionen unterstützen einige Programme beide Methoden zur Verschlüsselung Ihrer Amazon EBS-Volumes, während andere nur vom Kunden verwaltete Schlüssel unterstützen.

Weitere Informationen, wo diese Funktion noch nicht unterstützt wird, finden Sie unter China Regions

In der folgenden Liste wird der Schlüssel beschrieben, der GuardDuty verwendet, unabhängig davon, ob Ihre Amazon EBS-Volumes verschlüsselt sind oder nicht:

- Amazon EBS-Volumes, die entweder unverschlüsselt oder mit verschlüsselt sind Von AWS verwalteter Schlüssel — GuardDuty verwendet einen eigenen Schlüssel, um die replizierten Amazon EBS-Volumes zu verschlüsseln.

  Wenn Ihr Konto zu einem gehört AWS-Region , das das Scannen von Amazon EBS-Volumes nicht unterstützt, die mit der Standardeinstellung Von AWS verwalteter Schlüssel für EBS verschlüsselt sind, finden Sie unter. Ändern der AWS KMS Standardschlüssel-ID eines Amazon EBS-Volumes
- Amazon EBS-Volumes, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind — GuardDuty verwendet denselben Schlüssel, um das replizierte EBS-Volume zu verschlüsseln.

Malware Protection unterstützt das Scannen von Amazon EC2 EC2-Instances mit `productCode` as `marketplace` nicht. Wenn ein Malware-Scan für eine solche Amazon-EC2-Instance initiiert wird, wird der Scan übersprungen. Weitere Informationen finden Sie unter `UNSUPPORTED_PRODUCT_CODE_TYPE` in Gründe für das Überspringen von Ressourcen beim Malware-Scan.

Ändern der AWS KMS Standardschlüssel-ID eines Amazon EBS-Volumes

Standardmäßig wird beim Aufrufen der CreateVolumeAPI mit eingestellter Verschlüsselung `true` und ohne Angabe der KMS-Schlüssel-ID ein Amazon EBS-Volume erstellt, das mit dem AWS KMS Standardschlüssel für die EBS-Verschlüsselung verschlüsselt wird. Wenn ein Verschlüsselungsschlüssel jedoch nicht explizit angegeben wird, können Sie den Standardschlüssel ändern, indem Sie die ModifyEbsDefaultKmsKeyIdAPI aufrufen oder den entsprechenden Befehl verwenden. AWS CLI

Um die EBS-Standardschlüssel-ID zu ändern, fügen Sie Ihrer IAM-Richtlinie die folgende erforderliche Berechtigung hinzu: `ec2:modifyEbsDefaultKmsKeyId`. Jedes neu erstellte Amazon EBS-Volume, das Sie für die Verschlüsselung auswählen, aber keine zugehörige KMS-Schlüssel-ID angeben, verwendet die Standardschlüssel-ID. Verwenden Sie eine der folgenden Methoden, um die EBS-Standardschlüssel-ID zu aktualisieren:

So ändern Sie die standardmäßige KMS-Schlüssel-ID eines Amazon-EBS-Volumes

Führen Sie eine der folgenden Aktionen aus:

- Verwenden einer API — Sie können die ModifyEbsDefaultKmsKeyIdAPI verwenden. Informationen darüber, wie Sie den Verschlüsselungsstatus Ihres Volumes anzeigen können, finden Sie unter Amazon EBS-Volume erstellen.
- AWS CLI Befehl verwenden — Im folgenden Beispiel wird die standardmäßige KMS-Schlüssel-ID geändert, mit der Amazon EBS-Volumes verschlüsselt werden, wenn Sie keine KMS-Schlüssel-ID angeben. Achten Sie darauf, die Region durch die Ihrer AWS-Region KM-Schlüssel-ID zu ersetzen.

```
aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-
id AKIAIOSFODNN7EXAMPLE
```

Der obige Befehl wird eine Ausgabe erzeugen, die folgendermaßen aussieht:

```
{
```

```
  "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"
}
```

Weitere Informationen finden Sie unter modify-ebs-default-kms-key-id.

Anpassungen in Malware Protection

In diesem Abschnitt wird beschrieben, wie Sie die Scanoptionen für Ihre Amazon EC2 EC2-Instances oder Container-Workloads anpassen können, wenn ein Malware-Scan aufgerufen wird, entweder bei Bedarf oder über. GuardDuty

Allgemeine Einstellungen

Snapshot-Beibehaltung

GuardDuty bietet Ihnen die Möglichkeit, die Snapshots Ihrer EBS-Volumes in Ihrem Konto zu speichern. AWS Standardmäßig ist die Aufbewahrungseinstellung für Snapshots deaktiviert. Die Snapshots werden nur beibehalten, wenn Sie diese Einstellung aktiviert haben, bevor der Scan gestartet wird.

Wenn der Scan gestartet wird, werden die Replikat-EBS-Volumes auf der Grundlage der Snapshots Ihrer EBS-Volumes GuardDuty generiert. Nachdem der Scan abgeschlossen ist und die Einstellung zur Aufbewahrung von Snapshots in Ihrem Konto bereits aktiviert wurde, werden die Snapshots Ihrer EBS-Volumes nur beibehalten, wenn Malware gefunden und Erkenntnistypen für Malware Protection generiert wird. Unabhängig davon, ob Sie die Einstellung zur Aufbewahrung von Snapshots aktiviert haben oder nicht, werden die Snapshots Ihrer EBS-Volumes GuardDuty automatisch gelöscht, wenn keine Malware erkannt wird.

Nutzungskosten für Snapshots

Während des Malware-Scans, bei dem die Snapshots Ihrer Amazon EBS-Volumes GuardDuty erstellt werden, fallen mit diesem Schritt Nutzungskosten an. Wenn Sie die Einstellung zur Aufbewahrung von Snapshots für Ihr Konto aktivieren, fallen für Sie Nutzungskosten an, wenn Malware gefunden wird und die Snapshots beibehalten werden. Informationen zu den Kosten von Snapshots und deren Beibehaltung finden Sie unter Amazon-EBS-Preise.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die Aufbewahrungseinstellung für Snapshots zu aktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich unter Schutzpläne die Option Malware Protection.
3. Wählen Sie im unteren Bereich der Konsole Allgemeine Einstellungen. Um die Snapshots beizubehalten, aktivieren Sie die Option Beibehaltung von Snapshots.

API/CLI

1. Führen Sie den UpdateMalwareScanSettingsBefehl aus, um die aktuelle Konfiguration für die Einstellung zur Aufbewahrung von Snapshots zu aktualisieren.
2. Alternativ können Sie den folgenden AWS CLI Befehl ausführen, um Snapshots automatisch beizubehalten, wenn GuardDuty Malware Protection Ergebnisse generiert.

   Stellen Sie sicher, dass Sie die *`Detektor-ID`* durch Ihre eigene gültige `detectorId` ersetzen.
3. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ - Konsole.

   ```
   aws guardduty update-malware-scan-settings --detector-
   id 60b87779336485625 54d637e0e4bb3b2 --ebs-snapshot-preservation
    "RETENTION_WITH_FINDING"
   ```
4. Wenn Sie die Beibehaltung von Snapshots deaktivieren möchten, ersetzen Sie sie `RETENTION_WITH_FINDING` durch `NO_RETENTION`.

Scan-Optionen mit benutzerdefinierten Tags

Mithilfe des GuardDuty -initiierten Malware-Scans können Sie auch Tags angeben, um Amazon EC2-Instances und Amazon EBS-Volumes vom Scan- und Bedrohungserkennungsprozess entweder ein- oder auszuschließen. Sie können jeden GuardDuty -initiierten Malware-Scan individuell anpassen, indem Sie die Tags entweder in der Liste der Inklusions- oder Ausschlusstags bearbeiten. Jede Liste kann bis zu 50 Tags enthalten.

Falls Ihren EC2-Ressourcen noch keine benutzerdefinierten Tags zugeordnet sind, finden Sie weitere Informationen unter Markieren Ihrer Amazon-EC2-Ressourcen im Amazon-EC2-

Benutzerhandbuch für Linux-Instances oder Markieren Ihrer Amazon-EC2-Ressourcen im Amazon-EC2-Benutzerhandbuch für Windows-Instances.

> **Note**
>
> Der Malware-Scan auf Abruf unterstützt keine Scan-Optionen mit benutzerdefinierten Tags. Er unterstützt Globales `GuardDutyExcluded`-Tag.

So schließen Sie EC2-Instances vom Malware-Scan aus

Wenn Sie während des Scanvorgangs eine Amazon EC2 EC2-Instance oder ein Amazon EBS-Volume ausschließen möchten, können Sie das `GuardDutyExcluded` Tag `true` für jede Amazon EC2 EC2-Instance oder jedes Amazon EBS-Volume auf setzen und es GuardDuty wird nicht gescannt. Weitere Informationen über das `GuardDutyExcluded`-Tag finden Sie unter Serviceverknüpfte Rollenberechtigungen für den Malware Protection. Sie können auch ein Amazon-EC2-Instance-Tag zu einer Ausschlussliste hinzufügen. Wenn Sie der Liste der Ausschluss-Tags mehrere Tags hinzufügen, wird jede Amazon-EC2-Instance, die mindestens eines dieser Tags enthält, vom Malware-Scanvorgang ausgeschlossen.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um ein mit einer Amazon-EC2-Instance verknüpftes Tag zu einer Ausschlussliste hinzuzufügen.

Console

1. Öffnen Sie die Konsole unter https://console.aws.amazon.com/guardduty/ GuardDuty .
2. Wählen Sie im Navigationsbereich unter Schutzpläne die Option Malware Protection.
3. Erweitern Sie den Abschnitt Einschluss-/Ausschluss-Tags. Wählen Sie Tags hinzufügen aus.
4. Wählen Sie Ausschluss-Tags und anschließend Bestätigen.
5. Geben Sie das **`Key`**- und **`Value`**-Paar des Tags an, das Sie ausschließen möchten. Die Angabe von **`Value`** ist optional. Nachdem Sie alle Tags hinzugefügt haben, wählen Sie Speichern.

   > **Important**
   >
   > Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie unter Tag-Einschränkungen im

Amazon-EC2-Benutzerhandbuch für Linux-Instances oder Tag-Einschränkungen im Amazon-EC2-Benutzerhandbuch für Windows-Instances.

Wenn kein Wert für einen Schlüssel angegeben wird und die EC2-Instance mit dem angegebenen Schlüssel gekennzeichnet ist, wird diese EC2-Instance unabhängig vom zugewiesenen Wert des Tags vom GuardDuty -initiierten Malware-Scanvorgang ausgeschlossen.

API/CLI

- Aktualisieren Sie die Einstellungen für den Malware-Scan, indem Sie eine EC2-Instance oder einen Container-Workload vom Scanvorgang ausschließen.

  Mit dem folgenden AWS CLI Beispielbefehl wird der Liste der Ausschlusstags ein neues Tag hinzugefügt. Stellen Sie sicher, dass Sie die *`Detektor-ID`* durch Ihre eigene gültige `detectorId` ersetzen.

  `MapEquals` ist eine Liste von `Key`/`Value`-Paaren.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Exclude":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

  Important

  Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie unter Tag-Einschränkungen im Amazon-EC2-Benutzerhandbuch für Linux-Instances oder Tag-Einschränkungen im Amazon-EC2-Benutzerhandbuch für Windows-Instances.

So schließen Sie EC2-Instances in den Malware-Scan ein

Wenn Sie eine EC2-Instance scannen möchten, fügen Sie ihr Tag zur Einschluss-Liste hinzu. Wenn Sie ein Tag zu einer Liste mit Einschluss-Tags hinzufügen, wird eine EC2-Instance, die keines der hinzugefügten Tags enthält, aus dem Malware-Scan übersprungen. Wenn Sie der Liste der Einschluss-Tags mehrere Tags hinzufügen, wird eine EC2-Instance, die mindestens eines dieser Tags enthält, in den Malware-Scan aufgenommen. Manchmal kann es vorkommen, dass eine EC2-Instance während des Scanvorgangs übersprungen wird. Weitere Informationen finden Sie unter Gründe für das Überspringen von Ressourcen beim Malware-Scan.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um ein mit einer Amazon-EC2-Instance verknüpftes Tag zu einer Einschlussliste hinzuzufügen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich unter Schutzpläne die Option Malware Protection.
3. Erweitern Sie den Abschnitt Einschluss-/Ausschluss-Tags. Wählen Sie Tags hinzufügen aus.
4. Wählen Sie Einschluss-Tags und dann Bestätigen.
5. Wählen Sie Neues Einschluss-Tag hinzufügen und geben Sie das **`Key`**- und **`Value`**-Paar des Tags an, das Sie einbeziehen möchten. Die Angabe von **`Value`** ist optional.

   Nachdem Sie alle Einschluss-Tags hinzugefügt haben, wählen Sie Speichern.

   Wenn kein Wert für einen Schlüssel angegeben wird und eine EC2-Instance mit dem angegebenen Schlüssel markiert ist, wird die EC2-Instance in den Scanvorgang von Malware Protection einbezogen, unabhängig vom zugewiesenen Wert des Tags.

API/CLI

- Aktualisieren Sie die Einstellungen für den Malware-Scan, um eine EC2-Instance oder einen Container-Workload in den Scanvorgangs einzuschliessen.

  Mit dem folgenden AWS CLI Beispielbefehl wird der Liste der Inclusion-Tags ein neues Tag hinzugefügt. Stellen Sie sicher, dass Sie die *`Detektor-ID`* durch Ihre eigene gültige `detectorId` ersetzen. Ersetzen Sie das Beispiel *`TestKey`*und *`TestValue`*durch das `Value` Paar `Key` und des Tags, das mit Ihrer EC2-Ressource verknüpft ist.

`MapEquals` ist eine Liste von `Key`/`Value`-Paaren.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625554d637e0e4bb3b2 --scan-resource-criteria '{"Include":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

> **Important**
>
> Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie unter Tag-Einschränkungen im Amazon-EC2-Benutzerhandbuch für Linux-Instances oder Tag-Einschränkungen im Amazon-EC2-Benutzerhandbuch für Windows-Instances.

> **Note**
>
> Es kann bis zu 5 Minuten dauern GuardDuty , bis ein neues Tag erkannt wird.

Sie können jederzeit entweder Einschluss-Tags oder Ausschluss-Tags wählen, aber nicht beides. Wenn Sie zwischen den Tags wechseln möchten, wählen Sie dieses Tag aus dem Drop-down-Menü aus, wenn Sie neue Tags hinzufügen, und Bestätigen Sie Ihre Auswahl. Diese Aktion löscht alle Ihre aktuellen Tags.

Globales **`GuardDutyExcluded`**-Tag

Standardmäßig werden die Snapshots Ihrer EBS-Volumes mit einem `GuardDutyScanId`-Tag erstellt. Entfernen Sie dieses Tag nicht, da dadurch der Zugriff auf die Snapshots GuardDuty verhindert wird. Beide Scantypen in Malware Protection scannen nicht die Amazon-EC2-Instances oder Amazon-EBS-Volumes, für die das `GuardDutyExcluded`-Tag auf `true` gesetzt ist. Wenn ein Malware Protection eine solche Ressource scannt, wird zwar eine Scan-ID generiert, der Scan

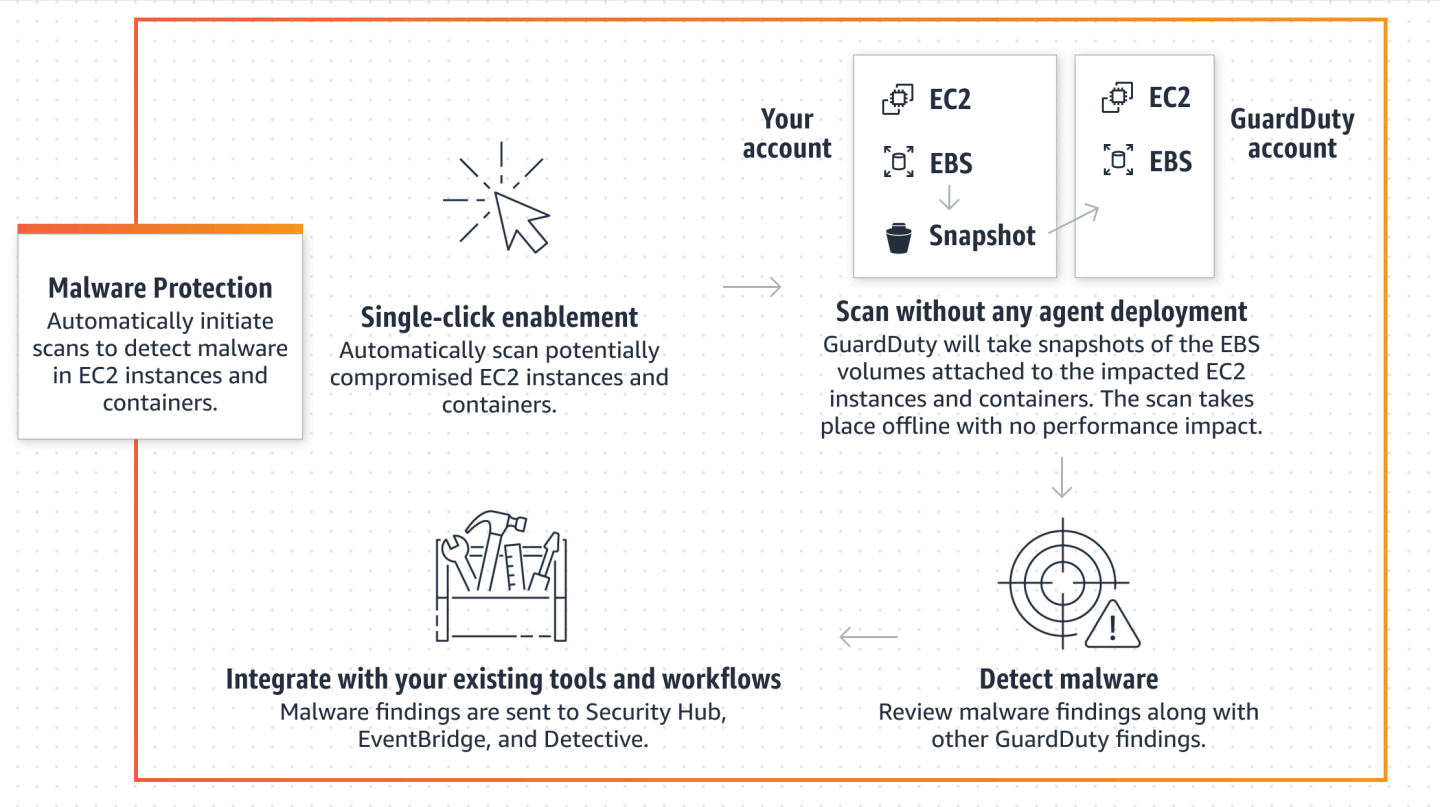
wird jedoch mit Angabe eines `EXCLUDED_BY_SCAN_SETTINGS`-Grunds übersprungen. Weitere Informationen finden Sie unter Gründe für das Überspringen von Ressourcen beim Malware-Scan.

GuardDuty-initiierter Malware-Scan

Wenn der GuardDuty -initiierte Malware-Scan aktiviert ist, wird bei jeder GuardDuty Erkennung bösartiger Aktivitäten, die auf das potenzielle Vorhandensein von Malware in Ihrer Amazon EC2 EC2-Instance- oder Container-Workload hinweisenErgebnisse, die einen GuardDuty -initiierten Malware-Scan auslösen, GuardDuty automatisch ein agentenloser Scan auf den Amazon Elastic Block Store (Amazon EBS) -Volumes initiiert, die an die potenziell betroffene Amazon EC2 EC2-Instance oder Container-Workload angehängt sind, um das Vorhandensein von Malware zu erkennen. GuardDuty Mit den Scan-Optionen können Sie Einschluss-Tags hinzufügen, die mit den Ressourcen verknüpft sind, die Sie scannen möchten, oder Ausschluss-Tags hinzufügen, die mit den Ressourcen verknüpft sind, die Sie aus dem Scanvorgang auslassen möchten. Bei der automatischen Initiierung des Scans werden immer Ihre Scan-Optionen berücksichtigt. Sie können auch die Einstellung zur Beibehaltung von Snapshots aktivieren, sodass die Snapshots Ihrer EBS-Volumes nur dann gespeichert werden, wenn der Malware Protection das Vorhandensein von Malware erkennt. Weitere Informationen finden Sie unter Anpassungen in Malware Protection.

Für jede Amazon EC2 EC2-Instance und Container-Workload, für die Ergebnisse GuardDuty generiert werden, wird einmal alle 24 Stunden ein automatisch GuardDuty initiierter Malware-Scan aufgerufen. Informationen darüber, wie die Amazon-EBS-Volumes gescannt werden, die Ihrer Amazon-EC2-Instance oder Ihrem Container-Workload zugeordnet sind, finden Sie unter Feature in Malware Protection.

Die folgende Abbildung beschreibt, wie der GuardDuty -initiierte Malware-Scan funktioniert.



GuardDuty GeneriertErkenntnistypen für Malware Protection, wenn Malware gefunden wird. Wenn GuardDuty kein Ergebnis generiert wird, das auf Malware auf derselben Ressource hinweist, wird kein GuardDuty -initiierter Malware-Scan ausgeführt. Sie können auf derselben Ressource auch einen Malware-Scan auf Abruf starten. Weitere Informationen finden Sie unter Malware-Scan auf Abruf.

Wie wirkt sich eine 30-tägige kostenlose Testphase auf Konten aus GuardDuty

Sie können die von uns GuardDuty initiierte Malware-Scan-Funktion für jedes Konto oder für jedes verfügbare AWS-Regionen Konto jederzeit ein- oder ausschalten.

- GuardDuty Bei der ersten Aktivierung (neues GuardDuty Konto) ist der GuardDuty -initiierte Malware-Scan bereits aktiviert und in der 30-tägigen kostenlosen Testphase enthalten.
- Die vorhandenen GuardDuty Konten können den GuardDuty -initiierten Malware-Scan im Rahmen einer 30-tägigen kostenlosen Testphase zum ersten Mal aktivieren.
- Wenn Sie bereits über ein GuardDuty Konto verfügen, das den Malware-Schutz verwendet hat, bevor der On-Demand-Malware-Scan allgemein verfügbar war, und für dieses GuardDuty Konto bereits das Preismodell gilt, sind keine Maßnahmen erforderlich AWS-Region, um den GuardDuty -initiierten Malware-Scan weiterhin zu verwenden.

> **Note**
>
> Wenn Sie eine 30-tägige kostenlose Testphase abgeschlossen haben, fallen die Nutzungskosten für die Erstellung der Amazon-EBS-Volume-Snapshots und deren Beibehaltung weiterhin an. Weitere Informationen finden Sie unter Amazon EBS – Preise.

Informationen zur Aktivierung des durch den Benutzer GuardDuty initiierten Malware-Scans finden Sie unter. Konfiguration des GuardDuty -initiierten Malware-Scans

Konfiguration des GuardDuty -initiierten Malware-Scans

Konfiguration des GuardDuty -initiierten Malware-Scans für ein eigenständiges Konto

Für Konten, die mit verknüpft sind AWS Organizations, können Sie diesen Vorgang über die Konsoleneinstellungen automatisieren, wie im nächsten Abschnitt beschrieben.

Um den GuardDuty -initiierten Malware-Scan zu aktivieren oder zu deaktivieren

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty -initiierten Malware-Scan für ein eigenständiges Konto zu konfigurieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich unter Schutzpläne die Option Malware Protection.
3. Im Bereich Malware-Schutz wird der aktuelle Status des GuardDuty -initiierten Malware-Scans für Ihr Konto aufgeführt. Sie können das jederzeit aktivieren oder deaktivieren, indem Sie Aktivieren oder Deaktivieren auswählen.
4. Wählen Sie Speichern.

API/CLI

- Führen Sie den API-Vorgang updateDetector aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `dataSources`-Objektnamen mit `EbsVolumes` auf `true` oder `false` setzen.

Sie können den GuardDuty -initiierten Malware-Scan auch mithilfe von Befehlszeilentools aktivieren oder deaktivieren, indem Sie den folgenden AWS AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie Ihre eigene gültige *Detektor-ID* verwenden.

> **Note**
>
> Der folgende Beispielcode aktiviert den GuardDuty -initiierten Malware-Scan. Um die Funktion zu deaktivieren, ersetzen Sie `true` durch `false`.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
 aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "EBS_MALWARE_PROTECTION", "Status" : "ENABLED"}]'
```

Konfiguration des GuardDuty -initiierten Malware-Scans in Umgebungen mit mehreren Konten

In einer Umgebung mit mehreren Konten können nur GuardDuty Administratorkonten den -initiierten Malware-Scan konfigurieren. GuardDuty GuardDuty Administratorkonten können die Verwendung von GuardDuty -initiiertem Malware-Scan für ihre Mitgliedskonten aktivieren oder deaktivieren. Sobald das Administratorkonto den GuardDuty -initiierten Malware-Scan für ein Mitgliedskonto konfiguriert hat, folgt das Mitgliedskonto den Einstellungen des Administratorkontos und kann diese Einstellungen nicht über die Konsole ändern. GuardDuty Administratorkonten, die ihre Mitgliedskonten beim AWS Organizations Support verwalten, können festlegen, dass der GuardDuty -initiierte Malware-Scan automatisch für alle vorhandenen und neuen Konten in der Organisation aktiviert wird. Weitere Informationen finden Sie unter GuardDuty Konten verwalten mit AWS Organizations.

Einrichtung eines vertrauenswürdigen Zugriffs zur Aktivierung des GuardDuty -initiierten Malware-Scans

Wenn das GuardDuty delegierte Administratorkonto nicht mit dem Verwaltungskonto in Ihrer Organisation identisch ist, muss das Verwaltungskonto den GuardDuty -initiierten Malware-Scan für die Organisation aktivieren. Auf diese Weise kann das delegierte Administratorkonto die

Serviceverknüpfte Rollenberechtigungen für den Malware Protection internen Mitgliedskonten erstellen, über die verwaltet werden. AWS Organizations

> **Note**
>
> Bevor Sie ein delegiertes GuardDuty Administratorkonto festlegen, finden Sie weitere Informationen unter. Überlegungen und Empfehlungen

Wählen Sie Ihre bevorzugte Zugriffsmethode, damit das delegierte GuardDuty Administratorkonto die von Ihnen GuardDuty initiierte Malware-Suche für Mitgliedskonten in der Organisation aktivieren kann.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Verwenden Sie das Verwaltungskonto Ihrer AWS Organizations Organisation, um sich anzumelden.

2. a. Wenn Sie kein delegiertes GuardDuty Administratorkonto angegeben haben, gehen Sie wie folgt vor:

      Geben Sie auf der Seite Einstellungen unter Delegiertes GuardDuty Administratorkonto die 12-stellige Zahl ein, **`account ID`** die Sie für die Verwaltung der GuardDuty Richtlinie in Ihrer Organisation angeben möchten. Wählen Sie Delegieren.

   b. i. Wenn Sie bereits ein delegiertes GuardDuty Administratorkonto festgelegt haben, das sich vom Verwaltungskonto unterscheidet, gehen Sie wie folgt vor:

         Aktivieren Sie auf der Seite Einstellungen unter Delegierter Administrator die Einstellung Berechtigungen. Diese Aktion ermöglicht es dem delegierten GuardDuty Administratorkonto, den Mitgliedskonten entsprechende Berechtigungen zuzuweisen und die von ihnen GuardDuty initiierte Malware-Suche in diesen Mitgliedskonten zu aktivieren.

      ii. Wenn Sie bereits ein delegiertes GuardDuty Administratorkonto eingerichtet haben, das mit dem Verwaltungskonto identisch ist, können Sie den GuardDuty -initiierten Malware-Scan für die Mitgliedskonten direkt aktivieren. Weitere Informationen finden Sie unter Automatische Aktivierung des GuardDuty -initiierten Malware-Scans für alle Mitgliedskonten.

> **Tip**
>
> Wenn sich das delegierte GuardDuty Administratorkonto von Ihrem Verwaltungskonto unterscheidet, müssen Sie dem delegierten GuardDuty Administratorkonto Berechtigungen zuweisen, um die Aktivierung des GuardDuty -initiierten Malware-Scans für Mitgliedskonten zu ermöglichen.

3. Wenn Sie dem delegierten GuardDuty Administratorkonto erlauben möchten, den GuardDuty -initiierten Malware-Scan für Mitgliedskonten in anderen Regionen zu aktivieren, ändern Sie Ihr Konto und wiederholen Sie die AWS-Region obigen Schritte.

API/CLI

1. Mit den Anmeldeinformationen für Ihr Verwaltungskonto führen Sie den folgenden Befehl aus:

```
aws organizations enable-aws-service-access --service-principal malware-
protection.guardduty.amazonaws.com
```

2. (Optional) Um den GuardDuty -initiierten Malware-Scan für das Verwaltungskonto zu aktivieren, bei dem es sich nicht um ein delegiertes Administratorkonto handelt, erstellt das Verwaltungskonto zuerst das Serviceverknüpfte Rollenberechtigungen für den Malware Protection explizit in seinem Konto und aktiviert dann den GuardDuty -initiierten Malware-Scan vom delegierten Administratorkonto aus, ähnlich wie bei jedem anderen Mitgliedskonto.

```
aws iam create-service-linked-role --aws-service-name malware-
protection.guardduty.amazonaws.com
```

3. Sie haben das delegierte GuardDuty Administratorkonto im aktuell ausgewählten Konto angegeben. AWS-Region Wenn Sie in einer Region ein Konto als delegiertes GuardDuty Administratorkonto festgelegt haben, muss dieses Konto Ihr delegiertes GuardDuty Administratorkonto in allen anderen Regionen sein. Wiederholen Sie den obigen Schritt für alle anderen Regionen.

Konfiguration des GuardDuty -initiierten Malware-Scans für das delegierte Administratorkonto GuardDuty

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty -initiierten Malware-Scan für ein GuardDuty delegiertes Administratorkonto zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen des Verwaltungskontos verwenden.
2. Wählen Sie im Navigationsbereich Malware Protection.
3. Wählen Sie auf der Seite Malware-Schutz neben GuardDuty-initiierter Malware-Scan die Option Bearbeiten aus.
4. Führen Sie eine der folgenden Aktionen aus:

   Verwendung von Für alle Konten aktivieren

   - Wählen Sie Für alle Konten aktivieren. Dadurch wird der Schutzplan für alle aktiven GuardDuty Konten in Ihrer AWS Organisation aktiviert, einschließlich der neuen Konten, die der Organisation beitreten.
   - Wählen Sie Speichern.

   Verwendung von Konten manuell konfigurieren

   - Um den Schutzplan nur für das delegierte GuardDuty Administratorkonto zu aktivieren, wählen Sie Konten manuell konfigurieren.
   - Wählen Sie im Abschnitt für das delegierte GuardDuty Administratorkonto (dieses Konto) die Option Aktivieren aus.
   - Wählen Sie Speichern.

API/CLI

Führen Sie den API-Vorgang updateDetector aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen `name` als `EBS_MALWARE_PROTECTION` und `status` als `ENABLED` oder `DISABLED` übergeben.

Sie können den GuardDuty -initiierten Malware-Scan aktivieren oder deaktivieren, indem Sie den folgenden AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie die gültige *Detektor-ID* des delegierten GuardDuty Administratorkontos verwenden.

> **Note**
>
> Der folgende Beispielcode aktiviert den GuardDuty -initiierten Malware-Scan. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /
              --account-ids 555555555555 /
              --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Automatische Aktivierung des GuardDuty -initiierten Malware-Scans für alle Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die GuardDuty -initiierte Malware-Scan-Funktion für alle Mitgliedskonten zu aktivieren. Dazu gehören der delegierte Administrator, bestehende Mitgliedskonten und die neuen Konten, die der Organisation beitreten.

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.

2. Führen Sie eine der folgenden Aktionen aus:

   Verwenden Sie die Seite Malware Protection

   1. Wählen Sie im Navigationsbereich Malware Protection.
   2. Wählen Sie auf der Seite Malware-Schutz im Abschnitt GuardDuty-initiierter Malware-Scan die Option Bearbeiten aus.

3. Wählen Sie Für alle Konten aktivieren. Diese Aktion aktiviert automatisch den GuardDuty -initiierten Malware-Scan sowohl für bestehende als auch für neue Konten in der Organisation.
4. Wählen Sie Speichern.

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Verwenden der Seite Konten

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren und anschließend Konten auf Einladung hinzufügen.
3. Wählen Sie im Fenster „Einstellungen für automatische Aktivierung verwalten“ die Option „Für alle Konten unter GuardDuty-initiiertem Malware-Scan aktivieren“ aus.
4. Wählen Sie auf der Seite Malware-Schutz im Bereich GuardDuty-initiierter Malware-Scan die Option Bearbeiten aus.
5. Wählen Sie Für alle Konten aktivieren. Diese Aktion aktiviert automatisch den GuardDuty -initiierten Malware-Scan sowohl für bestehende als auch für neue Konten in der Organisation.
6. Wählen Sie Speichern.

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Verwenden der Seite Konten

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren und anschließend Konten auf Einladung hinzufügen.

3. Wählen Sie im Fenster „Einstellungen für automatische Aktivierung verwalten“ die Option „Für alle Konten unter GuardDuty-initiiertem Malware-Scan aktivieren“ aus.
4. Wählen Sie Speichern.

Falls Sie die Option Für alle Konten aktivieren nicht verwenden können, finden Sie weitere Informationen unter Aktiviere oder deaktiviere selektiv den GuardDuty -initiierten Malware-Scan für Mitgliedskonten.

API/CLI

- *Um den GuardDuty -initiierten Malware-Scan für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den updateMemberDetectorsAPI-Vorgang mit Ihrer eigenen Detektor-ID auf.*
- Das folgende Beispiel zeigt, wie Sie den GuardDuty -initiierten Malware-Scan für ein einzelnes Mitgliedskonto aktivieren können. Um ein Mitgliedskonto zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
  ```

  Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.
- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivieren Sie den GuardDuty -initiierten Malware-Scan für alle vorhandenen aktiven Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty -initiierten Malware-Scan für alle vorhandenen aktiven Mitgliedskonten in der Organisation zu aktivieren.

So konfigurieren Sie den GuardDuty -initiierten Malware-Scan für alle vorhandenen aktiven Mitgliedskonten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldeinformationen für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich Malware Protection.
3. Im Malware-Schutz können Sie den aktuellen Status der GuardDuty-initiierten Malware-Scan-Konfiguration einsehen. Wählen Sie im Abschnitt Aktive Mitgliedskonten die Option Aktionen.
4. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
5. Wählen Sie Speichern.

Automatische Aktivierung des GuardDuty -initiierten Malware-Scans für neue Mitgliedskonten

Die neu hinzugefügten Mitgliedskonten müssen aktiviert werden, GuardDuty bevor die Konfiguration des GuardDuty -initiierten Malware-Scans ausgewählt werden kann. Die auf Einladung verwalteten Mitgliedskonten können den GuardDuty -initiierten Malware-Scan für ihre Konten manuell konfigurieren. Weitere Informationen finden Sie unter Step 3 - Accept an invitation.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty -initiierten Malware-Scan für neue Konten zu aktivieren, die Ihrer Organisation beitreten.

Console

Das delegierte GuardDuty Administratorkonto kann den GuardDuty -initiierten Malware-Scan für neue Mitgliedskonten in einer Organisation entweder über die Seite Malware-Schutz oder Konten aktivieren.

So aktivieren Sie automatisch den GuardDuty -initiierten Malware-Scan für neue Mitgliedskonten

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Führen Sie eine der folgenden Aktionen aus:

- Verwenden der Seite Malware Protection:

  1. Wählen Sie im Navigationsbereich Malware Protection.
  2. Wählen Sie auf der Seite Malware-Schutz beim GuardDuty-initiierten Malware-Scan die Option Bearbeiten aus.
  3. Wählen Sie Konten manuell konfigurieren.
  4. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Durch diesen Schritt wird sichergestellt, dass jedes Mal, wenn ein neues Konto Ihrer Organisation beitritt, der von einem neuen Konto GuardDuty initiierte Malware-Scan automatisch für das Konto aktiviert wird. Nur das vom Unternehmen delegierte GuardDuty Administratorkonto kann diese Konfiguration ändern.
  5. Wählen Sie Speichern.

- Verwenden der Seite Konten:

  1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
  2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren.
  3. Wählen Sie im Fenster „Einstellungen für automatische Aktivierung verwalten“ die Option „Für neue Konten aktivieren“ unter „GuardDuty-initiierter Malware-Scan“ aus.
  4. Wählen Sie Speichern.

API/CLI

- *Um den GuardDuty -initiierten Malware-Scan für neue Mitgliedskonten zu aktivieren oder zu deaktivieren, rufen Sie den `UpdateOrganizationConfiguration`API-Vorgang mit Ihrer eigenen Detektor-ID auf.*
- Das folgende Beispiel zeigt, wie Sie den GuardDuty -initiierten Malware-Scan für ein einzelnes Mitgliedskonto aktivieren können. Informationen zur Deaktivierung finden Sie unter Aktiviere oder deaktiviere selektiv den GuardDuty -initiierten Malware-Scan für Mitgliedskonten. Wenn Sie es nicht für alle neuen Konten aktivieren möchten, die der Organisation beitreten, legen Sie die Einstellung `AutoEnable` auf `NONE` fest.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --AutoEnable --features '[{"Name":
 "EBS_MALWARE_PROTECTION", "AutoEnable": NEW}]'
```

Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktiviere oder deaktiviere selektiv den GuardDuty -initiierten Malware-Scan für Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty -initiierten Malware-Scan für Mitgliedskonten selektiv zu konfigurieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Prüfen Sie auf der Kontoseite in der Spalte „GuardDuty-initiierter Malware-Scan“ den Status Ihres Mitgliedskontos.
4. Wählen Sie das Konto aus, für das Sie den GuardDuty -initiierten Malware-Scan konfigurieren möchten. Sie können mehrere Konten gleichzeitig auswählen.
5. Wählen Sie im Menü Schutzpläne bearbeiten die entsprechende Option für den GuardDuty-initiierten Malware-Scan aus.

API/CLI

Um den GuardDuty -initiierten Malware-Scan für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den `updateMemberDetectors`API-Vorgang mit Ihrer eigenen Detektor-ID auf.

Das folgende Beispiel zeigt, wie Sie den GuardDuty -initiierten Malware-Scan für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION",
 "Status": "ENABLED"}]'
```

> **Note**
>
> Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Führen Sie den updateMemberDetectorsAPI-Vorgang mit Ihrer eigenen GuardDuty *Detektor-ID* aus, um den von Ihnen initiierten Malware-Scan selektiv für Ihre Mitgliedskonten zu aktivieren oder zu deaktivieren. Das folgende Beispiel zeigt, wie Sie den GuardDuty -initiierten Malware-Scan für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `true` durch `false`.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 123456789012 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

> **Note**
>
> Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto

Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivieren Sie den GuardDuty -initiierten Malware-Scan für bestehende Konten in der Organisation, die per Einladung verwaltet werden

Die mit dem Dienst verknüpfte Rolle (Service Linked Role, SLR) zum Schutz vor GuardDuty Schadsoftware muss in den Mitgliedskonten erstellt werden. Das Administratorkonto kann die Funktion „ GuardDuty-initiierter Malware-Scan“ nicht in Mitgliedskonten aktivieren, die nicht von verwaltet werden. AWS Organizations

Derzeit können Sie über die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/ die folgenden Schritte ausführen, um den GuardDuty -initiierten Malware-Scan für die vorhandenen Mitgliedskonten zu aktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldeinformationen Ihres Administratorkontos an.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Wählen Sie das Mitgliedskonto aus, für das Sie den GuardDuty -initiierten Malware-Scan aktivieren möchten. Sie können mehrere Konten gleichzeitig auswählen.
4. Wählen Sie Aktionen.
5. Wählen Sie Mitglied trennen.
6. Wählen Sie im Mitgliedskonto im Navigationsbereich Malware Protection unter Schutzpläne.
7. Wählen Sie „ GuardDuty-initiierten Malware-Scan aktivieren“. GuardDuty erstellt eine Spiegelreflexkamera für das Mitgliedskonto. Weitere Informationen zu SLR finden Sie unter Serviceverknüpfte Rollenberechtigungen für den Malware Protection.
8. Wählen Sie in Ihrem Administratorkonto im Navigationsbereich die Option Konten aus.
9. Wählen Sie das Mitgliedskonto aus, das der Organisation wieder hinzugefügt werden muss.
10. Wählen Sie Aktionen und dann Mitglied hinzufügen.

API/CLI

1. Verwenden Sie das Administratorkonto, um die DisassociateMembersAPI für die Mitgliedskonten auszuführen, die den GuardDuty -initiierten Malware-Scan aktivieren möchten.
2. Verwenden Sie Ihr Mitgliedskonto, um den GuardDuty -initiierten Malware-Scan aufzurufen und UpdateDetectorzu aktivieren.

   Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

   ```
   aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
   {"EbsVolumes":true}}}'
   ```

3. Verwenden Sie das Administratorkonto, um die CreateMembersAPI auszuführen, um das Mitglied wieder zur Organisation hinzuzufügen.

Ergebnisse, die einen GuardDuty -initiierten Malware-Scan auslösen

Ein GuardDuty -initiierter Malware-Scan wird ausgelöst, wenn verdächtiges Verhalten GuardDuty entdeckt wird, das auf Malware in Amazon EC2 EC2-Instance- oder Container-Workloads hindeutet.

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation

- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce (Nur ausgehend)
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/RDPBruteForce (Nur ausgehend)
- UnauthorizedAccess:EC2/SSHBruteForce (Nur ausgehend)
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay
- Backdoor:Runtime/C&CActivity.B
- Backdoor:Runtime/C&CActivity.B!DNS
- CryptoCurrency:Runtime/BitcoinTool.B
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Execution:Runtime/NewBinaryExecuted
- Execution:Runtime/NewLibraryLoaded
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/CryptoMinerExecuted
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DropPoint
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS
- UnauthorizedAccess:Runtime/MetadataDNSRebind

Malware-Scan auf Abruf

Der Malware-Scan auf Abruf hilft Ihnen, das Vorhandensein von Malware auf Amazon Elastic Block Store (Amazon EBS)-Volumes zu erkennen, die an Ihre Amazon-EC2-Instances angefügt sind. Sie können ohne Konfiguration einen Malware-Scan auf Abruf initiieren, indem Sie den Amazon-Ressourcennamen (ARN) der Amazon-EC2-Instance angeben, die Sie scannen möchten. Sie können einen On-Demand-Malware-Scan entweder über die Konsole oder die API initiieren. GuardDuty Bevor Sie einen Malware-Scan auf Abruf starten, können Sie Ihre bevorzugte Snapshot-Beibehaltung-Einstellung festlegen. Anhand der folgenden Szenarien können Sie ermitteln, wann Sie den Malware-Scan auf Abruf verwenden sollten GuardDuty:

- Sie möchten das Vorhandensein von Malware in Ihren Amazon EC2 EC2-Instances erkennen, ohne den GuardDuty -initiierten Malware-Scan zu aktivieren.
- Sie haben den GuardDuty -initiierten Malware-Scan aktiviert und ein Scan wurde automatisch gestartet. Wenn Sie die empfohlene Problembehebung für den generierten Erkenntnistyp von Malware Protection befolgt haben und einen Scan für dieselbe Ressource initiieren möchten, können Sie einen Malware-Scan auf Abruf starten, wenn 1 Stunde von der Startzeit des vorherigen Scans vergangen ist.

  Der Malware-Scan auf Abruf setzt nicht voraus, dass seit dem Zeitpunkt, an dem der vorherige Malware-Scan initiiert wurde, 24 Stunden vergangen sind. Es sollte eine Stunde vergangen sein,

bevor ein Malware-Scan auf Abruf auf derselben Ressource gestartet wird. Informationen dazu, wie Sie vermeiden können, dass ein Malware-Scan auf derselben EC2-Instance dupliziert wird, finden Sie unter Dieselbe Amazon-EC2-Instance erneut scannen.

> **Note**
>
> Der On-Demand-Malware-Scan ist in der 30-tägigen kostenlosen Testphase von nicht enthalten. GuardDuty Die Nutzungskosten beziehen sich auf das gesamte Amazon-EBS-Volumen, das bei jedem Malware-Scan gescannt wurde. Weitere Informationen finden Sie unter GuardDuty Amazon-Preise. Informationen zu den Kosten der Erstellung von Amazon-EBS-Volume-Snapshots und deren Aufbewahrung finden Sie unter Amazon-EBS-Preise.

So funktioniert der Malware-Scan auf Abruf

Mit dem Malware-Scan auf Abruf können Sie eine Malware-Scan-Anfrage für Ihre Amazon-EC2-Instance initiieren, auch wenn sie gerade verwendet wird. Nachdem Sie einen On-Demand-Malware-Scan initiiert haben, GuardDuty erstellt es Snapshots der Amazon EBS-Volumes, die an die Amazon EC2 EC2-Instance angehängt sind, deren Amazon Resource Name (ARN) für den Scan bereitgestellt wurde. Als Nächstes GuardDuty teilt diese Snapshots mit dem. GuardDuty Dienstkonto GuardDuty erstellt verschlüsselte EBS-Replikat-Volumes aus diesen Snapshots im Dienstkonto. GuardDuty Weitere Informationen dazu, wie Amazon-EBS-Volumes gescannt werden finden Sie unter Elastic Block Storage (EBS)-Volume.

> **Note**
>
> GuardDuty erstellt die Snapshots der Daten, die bereits auf die Amazon EBS-Volumes geschrieben wurden, point-in-time wenn Sie einen On-Demand-Malware-Scan starten.

Wenn Malware gefunden wird und Sie die Einstellung zur Aufbewahrung von Snapshots aktiviert haben, werden die Snapshots Ihrer EBS-Volumes nicht gelöscht und werden automatisch in Ihrem AWS-Konto gespeichert. Der Malware-Scan auf Abruf generiert die Erkenntnistypen für Malware Protection. Wenn keine Malware gefunden wird, werden die Snapshots Ihrer EBS-Volumes gelöscht, unabhängig von der Einstellung zur Beibehaltung von Snapshots.

Standardmäßig werden die Snapshots Ihrer EBS-Volumes mit einem `GuardDutyScanId`-Tag erstellt. Entfernen Sie dieses Tag nicht, da dadurch der Zugriff auf die GuardDuty Snapshots verhindert wird. Beide Scantypen in Malware Protection scannen nicht die Amazon-EC2-Instances oder Amazon-EBS-Volumes, für die das `GuardDutyExcluded`-Tag auf `true` gesetzt ist. Wenn ein Malware Protection eine solche Ressource scannt, wird zwar eine Scan-ID generiert, der Scan wird jedoch mit Angabe eines `EXCLUDED_BY_SCAN_SETTINGS`-Grunds übersprungen. Weitere Informationen finden Sie unter Gründe für das Überspringen von Ressourcen beim Malware-Scan.

AWS Organizations Richtlinie zur Dienststeuerung — Zugriff verweigert

Mithilfe der Service Control Policies (SCPs) in AWS Organizations kann das delegierte GuardDuty Administratorkonto Berechtigungen einschränken und Aktionen wie das Initiieren eines On-Demand-Malware-Scans für Amazon EC2 EC2-Instances, die Ihren Konten gehören, verweigern.

Als GuardDuty Mitgliedskonto erhalten Sie möglicherweise eine Fehlermeldung, wenn Sie einen On-Demand-Malware-Scan für Ihre Amazon EC2 EC2-Instances starten. Sie können sich mit dem Verwaltungskonto verbinden, um zu erfahren, warum ein SCP für Ihr Mitgliedskonto eingerichtet wurde. Weitere Informationen zu SCP-Auswirkungen auf Berechtigungen.

Erste Schritte mit dem Malware-Scan auf Abruf

Als GuardDuty Administratorkonto können Sie im Namen Ihrer aktiven Mitgliedskonten, für deren Konten die folgenden Voraussetzungen erfüllt sind, einen On-Demand-Malware-Scan initiieren. Eigenständige Konten und aktive Mitgliedskonten in GuardDuty können auch einen On-Demand-Malware-Scan für ihre eigenen Amazon EC2 EC2-Instances initiieren.

Voraussetzungen

- GuardDuty muss dort aktiviert sein, AWS-Regionen wo Sie den On-Demand-Malware-Scan starten möchten.
- Stellen Sie sicher, dass der AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess dem IAM-Benutzer oder der IAM-Rolle angefügt ist. Sie benötigen den Zugriffsschlüssel und den geheimen Schlüssel, die dem IAM-Benutzer oder der IAM-Rolle zugeordnet sind.
- Als delegiertes GuardDuty Administratorkonto haben Sie die Möglichkeit, im Namen eines aktiven Mitgliedskontos einen On-Demand-Malware-Scan zu initiieren.
- Wenn Sie ein Mitgliedskonto sind, das nicht über die Serviceverknüpfte Rollenberechtigungen für den Malware Protection verfügt, wird bei der Initiierung eines Malware-Scan auf Abruf für eine

Amazon-EC2-Instance, die zu Ihrem Konto gehört, automatisch die SLR für Malware Protection erstellt.

> **Important**
>
> Stellen Sie sicher, dass niemand die SLR-Berechtigungen für den Malware-Schutz löscht, solange der Malware-Scan, ob GuardDuty initiiert oder auf Anforderung, noch läuft. Dadurch wird verhindert, dass der Scan erfolgreich abgeschlossen wird und es wird kein definitives Scanergebnis angezeigt.

Bevor Sie einen Malware-Scan auf Abruf starten, stellen Sie sicher, dass in den letzten Stunde kein Scan auf derselben Ressource gestartet wurde. Andernfalls wird der Scan dedupliziert. Weitere Informationen finden Sie unter Dieselbe Ressource erneut scannen.

Starten eines Malware-Scans auf Abruf

Wählen Sie Ihre bevorzugte Zugriffsmethode, um einen Malware-Scan auf Abruf zu starten.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Initiieren Sie den Scanvorgang mithilfe einer der folgenden Optionen:
   a. Verwenden der Seite Malware Protection:
      i. Wählen Sie im Navigationsbereich unter Schutzpläne die Option Malware Protection.
      ii. Geben Sie auf der Seite Malware Protection den Amazon-EC2-Instance-ARN[1] an, für den Sie den Scan initiieren möchten.
   b. Verwendung der Seite Malware-Scans:
      i. Wählen Sie im Navigationsbereich Malware-Scans.
      ii. Wählen Sie Malware-Scan auf Abruf starten und geben Sie den Amazon-EC2-Instance ARN[1] an, für den Sie den Scan initiieren möchten.
      iii. Wenn es sich um einen Wiederholungs-Scan handelt, wählen Sie auf der Seite Malware-Scans eine Amazon-EC2-Instance-ID aus.

Erweitern Sie das Drop-down-Menü Scan auf Abruf starten und wählen Sie Ausgewählte Instance erneut scannen.

3. Nachdem Sie einen Scan mit einer der beiden Methoden erfolgreich initiiert haben, wird eine Scan-ID generiert. Sie können diese Scan-ID verwenden, um den Scan-Fortschritt zu verfolgen. Weitere Informationen finden Sie unter Überwachen von Scanstatus und Ergebnissen.

API/CLI

Rufen Sie auf StartMalwareScan, `resourceArn` der die Amazon EC2 EC2-Instance [1] akzeptiert, für die Sie einen On-Demand-Malware-Scan initiieren möchten.

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-
east-1:555555555555:instance/i-b188560f"
```

Nachdem Sie einen Scan erfolgreich initiiert haben, gibt `StartMalwareScan` `scanId` zurück. Invoke DescribeMalwareScansüberwacht den Fortschritt des initiierten Scans.

[1]Informationen zum Format Ihres Amazon-EC2-Instance-ARN finden Sie unter Amazon-Ressourcenname (ARN). Für Amazon-EC2-Instances können Sie das folgende ARN-Beispielformat verwenden, indem Sie die Werte für die Partition, Region, AWS-Konto -ID und Amazon-EC2-Instance-ID ersetzen. Informationen zur Länge Ihrer Instance-ID finden Sie unter Ressourcen-IDs.

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

Dieselbe Amazon-EC2-Instance erneut scannen

Unabhängig davon, ob ein Scan GuardDuty initiiert oder auf Anforderung ausgeführt wird, können Sie einen neuen On-Demand-Malware-Scan auf derselben EC2-Instance innerhalb einer Stunde ab dem Startzeitpunkt des vorherigen Malware-Scans starten. Wenn der neue Malware-Scan innerhalb von einer Stunde nach dem Start des vorherigen Malware-Scans initiiert wird, führt Ihre Anfrage zu dem folgenden Fehler, und es wird keine Scan-ID für diese Anfrage generiert.

```
A scan was initiated on this resource recently. You can request a scan on
the same resource one hour after the previous scan start time.
```

Informationen darüber, wie Sie einen neuen Scan für dieselbe Ressource starten, finden Sie unter Starten eines Malware-Scans auf Abruf.

Informationen zum Verfolgen des Status der Malware-Scans finden Sie unter Überwachung des Scanstatus und der Ergebnisse im Malware-Schutz GuardDuty .

Überwachung des Scanstatus und der Ergebnisse im Malware-Schutz GuardDuty

Sie können den Scanstatus jedes GuardDuty Malware-Schutz-Scans überwachen. Die möglichen Werte für den Scan-Status sind `Completed`, `Running`, `Skipped` und `Failed`.

Nach Abschluss des Scans wird das Scanergebnis für Scans mit dem Status `Completed` aufgefüllt. Mögliche Werte für das Scanergebnis sind `Clean` und `Infected`. Anhand des Scan-Typs können Sie feststellen, ob es sich bei dem Malware-Scan um `GuardDuty initiated` oder `On demand` handelte.

Die Scan-Ergebnisse für jeden Malware-Scan werden 90 Tage aufbewahrt. Wählen Sie Ihre bevorzugte Zugriffsmethode, um den Status Ihres Malware-Scans zu verfolgen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Malware-Scans.
3. Sie können die Malware-Scans anhand der folgenden Eigenschaften filtern, die in den Filterkriterien verfügbar sind.

   - Scan-ID
   - Konto-ID
   - EC2-Instance-ARN
   - Scan-Typ
   - Scan-Status

   Informationen zu Eigenschaften, die für Filterkriterien verwendet werden, finden Sie unter Erkenntnisdetails.

API/CLI

- Wenn für den Malware-Scan ein Scanergebnis vorliegt, können Sie die Malware-Scans auf der Grundlage von `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE`, `GUARDDUTY_FINDING_ID`, `SCAN_STATUS` und `SCAN_START_TIME` filtern.

  Die `GUARDDUTY_FINDING_ID` Filterkriterien sind verfügbar, wenn der GuardDuty initiiert `SCAN_TYPE` wird. Informationen zu allen Filterkriterien finden Sie unter Erkenntnisdetails.

- Sie können das Beispiel-*`Filterkriterium`* im folgenden Befehl ändern. Gegenwärtig können Sie auf der Grundlage von jeweils einem `CriterionKey` filtern. Die Optionen für `CriterionKey` sind `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE`, `GUARDDUTY_FINDING_ID`, `SCAN_STATUS` und `SCAN_START_TIME`.

  Wenn Sie dasselbe `CriterionKey` wie unten verwenden, stellen Sie sicher, dass Sie das Beispiel `EqualsValue` durch Ihre eigene gültige AWS -*`Scan-ID`* ersetzen.

  Ersetzen Sie das Beispiel `detector-id` durch Ihre eigene gültige *`detector-id`*. Sie können die *`maximalen Ergebnisse`* (bis zu 50) und die *`Sortierkriterien`* ändern. Der `AttributeName` ist verpflichtend und muss `scanStartTime` sein.

  ```
  aws guardduty describe-malware-scans --detector-
  id 60b87779336485625 54d637e0e4bb3b2 --max-results 1 --sort-criteria
   '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
   '{"FilterCriterion":[{"CriterionKey":"SCAN_ID", "FilterCondition":
  {"EqualsValue":"123456789012"}}] }'
  ```

- Die Antwort auf diesen Befehl zeigt maximal eine Erkenntnis mit Details zur betroffenen Ressource und zu den Malware-Erkenntnissen (wenn `Infected`) an.

GuardDuty Dienstkonten von AWS-Region

Wenn ein Snapshot erstellt und mit einem GuardDuty Dienstkonto geteilt wird, wird ein neues Ereignis in Ihren CloudTrail Protokollen erstellt. Dieses Ereignis spezifiziert das entsprechende `snapshotId` AND `userId` (GuardDuty Dienstkonto dafür AWS-Region). Weitere Informationen finden Sie unter Feature in Malware Protection.

Das folgende Beispiel ist ein Ausschnitt aus einem CloudTrail Ereignis, das den Anfragetext für die `ModifySnapshotAttribute` Anfrage anzeigt:

```
"requestParameters": {
        "snapshotId": "snap-1234567890abcdef0",
        "createVolumePermission": {
            "add": {
                "items": [
                    {
                        "userId": "111122223333"
                    }
                ]
            }
        },
        "attributeType": "CREATE_VOLUME_PERMISSION"
    }
```

Die folgende Tabelle zeigt die GuardDuty Dienstkonten für jede Region. Das `userId` ist das GuardDuty Dienstkonto und hängt von der ausgewählten Region ab.

AWS-Region	Regionscode	GuardDuty Dienstkonto-ID (**`userId`**)
USA Ost (Nord-Virginia)	us-east-1	652050842985
USA Ost (Ohio)	us-east-2	178123968615
USA West (Nordkali fornien)	us-west-1	669213148797
USA West (Oregon)	us-west-2	447226417196
Asien-Pazifik (Mumbai)	ap-south-1	913179291432
Asien-Pazifik (Osaka)	ap-northeast-3	089661699081
Asien-Pazifik (Seoul)	ap-northeast-2	039163547507
Asien-Pazifik (Tokio)	ap-northeast-1	874749492622
Asien-Pazifik (Singapur)	ap-southeast-1	247460962669
Asien-Pazifik (Sydney)	ap-southeast-2	124839743349
Kanada (Zentral)	ca-central-1	175877067165

AWS-Region	Regionscode	GuardDuty Dienstkonto-ID (**`userId`**)
Kanada West (Calgary)	ca-west-1	894794104037
Europa (Frankfurt)	eu-central-1	002294850712
Europa (Irland)	eu-west-1	283769539786
Europa (London)	eu-west-2	310125036783
Europa (Paris)	eu-west-3	866607715269
Europa (Stockholm)	eu-north-1	693780578038
China (Peking)	cn-north-1	448721096076
China (Ningxia)	cn-northwest-1	480864352451
Südamerika (São Paulo)	sa-east-1	546914126324
Asien-Pazifik (Hyderabad) (Opt-in)	ap-south-2	682251015962
Asien-Pazifik (Melbourne) (Opt-in)	ap-southeast-4	353488359550
Europa (Spanien) (Opt-In)	eu-south-2	936182149045
Europa (Zürich) (Opt-In)	eu-central-2	867642063380
Israel (Tel Aviv) (Opt-In)	il-central-1	619233833001
Europa (Mailand) (Opt-In)	eu-south-1	977238331021
Asien-Pazifik (Hongkong) (Opt-in)	ap-east-1	249472122084
Naher Osten (Bahrain) (Opt-In)	me-south-1	404001805210
Afrika (Kapstadt) (Opt-in)	af-south-1	957664736811

AWS-Region	Regionscode	GuardDuty Dienstkonto-ID (**`userId`**)
Asien-Pazifik (Jakarta) (Opt-in)	ap-southeast-3	452118225523
Naher Osten (VAE) (Opt-In)	me-central-1	828603743433

Kontingente für Malware Protection

Malware Protection bietet die folgende Standardverfügbarkeit verschiedener Ressourcen, die von dem Feature verwendet werden.

Scope	Standard	Kommentare
Extraktion und Analyse von Daten in komprimierten oder archivierten Dateien	5	Die maximale Anzahl von verschachtelten Ebenen, die in einer archivierten Datei zulässig sind.
Anzahl der Dateien in einer archivierten Datei	1000	Die maximale Anzahl an Dateien, die in einem Archiv gescannt werden können. Diese Anzahl ist die Summe der aus dem Archiv extrahier ten Dateien und der Anzahl der aus allen verschachtelten Archiven extrahierten Dateien.
Anzahl der Bedrohungen	32	Die maximale Anzahl von Bedrohungen, die Sie im Ergebnisfenster anzeigen können. GuardDuty Der Malware-Schutz hat möglicher weise mehr Bedrohung snamen erkannt. Wenn die Anzahl der erkannten

Scope	Standard	Kommentare
		Bedrohungsnamen höher als der Standardwert ist, können Sie die JSON-Deta ils anzeigen, indem Sie im Detailbereich der GuardDuty Konsole unter dem Namen des Befundes die Finding-ID auswählen.
Anzahl der Dateien pro erkannter Bedrohung	5	Die maximale Anzahl identifiz ierter Dateien pro erkannter Bedrohung. Wenn beispiels weise 10 Dateien GuardDuty erkannt werden, die mit einer einzigen Bedrohung verknüpft sind, zeigt die Bedrohung maximal 5 Dateien an.
EBS-Volumes pro Scan pro Instance	11	Die maximale Anzahl von EBS-Volumes, die pro EC2-Instance gescannt werden GuardDuty können. Wenn mehr als 11 EBS-Volumes gescannt werden müssen, sortiert GuardDuty Malware Protection sie `deviceName` alphabetisch und wählt die ersten 11 EBS-Volumes aus.

Scope	Standard	Kommentare
EBS-Volume-Größe	2048 GB	In Verbindung mit einer Amazon EC2 EC2-Instance und einem Container-Workload kann GuardDuty Malware Protection jedes Amazon EBS-Volume scannen, das bis zu 2048 GB groß ist. Dieses Kontingent gilt für alle, AWS-Region in denen die Unterstützung für Malware Protection verfügbar ist.
Unterstützte Dateitypen	GuardDuty Malware Protection kann die folgenden Dateisystemtypen scannen: • Dateisystem mit neuer Technologie (NTFS) • X-Dateisystem (XFS) • Zweites erweitertes Dateisystem (ext2) • Viertes erweitertes Dateisystem (ext4) • Dateisystem mit Dateizuordnungstabelle (FAT) • Virtuelles Dateisystem mit Dateizuordnungstabelle (VFAT)	NICHT ZUTREFFEND

Scope	Standard	Kommentare
Scan-Optionen-Tags	50	Die maximale Anzahl von Ressourcen-Tags, die Sie hinzufügen können, um die Einstellungen Ihrer Malware-Scan-Optionen anzupassen. Weitere Informationen finden Sie unter Scan-Optionen mit benutzerdefinierten Tags.
Aufbewahrungszeitraum für Ergebnisse	90	Die maximale Anzahl von Tagen, für die GuardDuty ein Ergebnis aufbewahrt wird. Die neuesten Informationen finden Sie unter Kontingente für Amazon GuardDuty.
Beibehaltungszeitraum für Malware-Scans	90	Die maximale Anzahl von Tagen, für die GuardDuty Malware Protection den Verlauf eines Scans aufbewahrt. Weitere Informationen zum Anzeigen der letzten Malware-Scans finden Sie unter Überwachung des Scanstatus und der Ergebnisse im Malware-Schutz GuardDuty .
Transaktionen pro Sekunde (TPS) für Malware-Scan auf Abruf	1	Die Anzahl der Anforderungen für Malware-Scan auf Abruf, die pro Sekunde in jeder Region initiiert werden können.

Scope	Standard	Kommentare
Burst-Limit für Malware-Scan auf Abruf	1	Die Anzahl der Anforderungen für Malware-Scan auf Abruf, die pro Sekunde in jeder Region initiiert werden können.

GuardDuty RDS-Schutz

RDS Protection in Amazon GuardDuty analysiert und profiliert RDS-Anmeldeaktivitäten im Hinblick auf potenzielle Zugriffsbedrohungen auf Ihre Amazon Aurora-Datenbanken (Amazon Aurora MySQL-kompatible Edition und Aurora PostgreSQL-kompatible Edition). Mit dieses Feature können Sie potenziell verdächtiges Anmeldeverhalten identifizieren. RDS Protection erfordert keine zusätzliche Infrastruktur und ist so konzipiert, dass die Leistung Ihrer Datenbank-Instances nicht beeinträchtigt wird.

Wenn RDS Protection einen potenziell verdächtigen oder anomalen Anmeldeversuch erkennt, der auf eine Bedrohung für Ihre Datenbank hindeutet, GuardDuty generiert RDS Protection ein neues Ergebnis mit Details über die potenziell gefährdete Datenbank.

Sie können die RDS-Schutzfunktion für jedes Konto an jedem Ort, AWS-Region an dem diese Funktion bei Amazon verfügbar ist GuardDuty, jederzeit aktivieren oder deaktivieren. Ein vorhandenes GuardDuty Konto kann RDS Protection mit einer 30-tägigen Testphase aktivieren. Für ein neues GuardDuty Konto ist RDS Protection bereits aktiviert und in der 30-tägigen kostenlosen Testphase enthalten. Weitere Informationen finden Sie unter Einschätzen der Kosten.

> **Note**
>
> Wenn die RDS-Schutzfunktion nicht aktiviert ist, werden GuardDuty weder Ihre RDS-Anmeldeaktivitäten erfasst noch ein ungewöhnliches oder verdächtiges Anmeldeverhalten erkannt.

Informationen darüber, AWS-Regionen wo RDS Protection noch GuardDuty nicht unterstützt wird, finden Sie unter. Verfügbarkeit regionsspezifischer Feature

Unterstützte Amazon-Aurora-Datenbanken

In der folgenden Tabelle wird die Unterstützung für Aurora-Datenbank-Versionen gezeigt.

Amazon-Aurora-DB-Engine	Unterstützte Engine-Versionen
Aurora MySQL	• 2.10.2 oder höher

Amazon-Aurora-DB-Engine	Unterstützte Engine-Versionen
	• 3.02.1 oder höher
Aurora PostgreSQL	• 10.17 oder höher • 11.12 oder höher • 12.7 oder höher • 13.3 oder höher • 14.3 oder höher • 15.2 oder höher • 16.1 oder später

So verwendet RDS Protection die Überwachung der RDS-Anmeldeaktivitäten

RDS Protection in Amazon GuardDuty hilft Ihnen, die unterstützten Amazon Aurora (Aurora) -Datenbanken in Ihrem Konto zu schützen. Nachdem Sie die RDS-Schutzfunktion aktiviert haben, beginnt GuardDuty sofort die Überwachung der RDS-Anmeldeaktivitäten aus den Aurora-Datenbanken in Ihrem Konto. GuardDuty überwacht kontinuierlich die RDS-Anmeldeaktivitäten und erstellt Profile für verdächtige Aktivitäten, z. B. unbefugten Zugriff auf die Aurora-Datenbank in Ihrem Konto durch einen zuvor unbekannten externen Akteur. Wenn Sie RDS Protection zum ersten Mal aktivieren oder eine neu erstellte Datenbank-Instance haben, ist eine Lernphase erforderlich, um das normale Verhalten als Grundlage zu nehmen. Aus diesem Grund kann es sein, dass neu aktivierte oder neu erstellte Datenbank-Instances bis zu zwei Wochen lang keine anomalen Anmelde-Erkenntnisse aufweisen. Weitere Informationen finden Sie unter Überwachung der RDS-Anmeldeaktivitäten.

Wenn RDS Protection eine potenzielle Bedrohung erkennt, z. B. ein ungewöhnliches Muster bei einer Reihe erfolgreicher, fehlgeschlagener oder unvollständiger Anmeldeversuche, GuardDuty generiert das System ein neues Ergebnis mit Details über die potenziell gefährdete Datenbank-Instance. Weitere Informationen finden Sie unter Erkenntnistypen für RDS Protection. Wenn Sie den RDS-Schutz deaktivieren, wird die Überwachung der RDS-Anmeldeaktivitäten GuardDuty sofort beendet und es kann keine potenzielle Bedrohung für Ihre unterstützten Datenbank-Instances erkannt werden.

> **Note**
>
> GuardDuty verwaltet Ihre Anmeldeaktivitäten Unterstützte Datenbanken oder RDS-Anmeldeaktivitäten nicht und stellt Ihnen auch keine RDS-Anmeldeaktivitäten zur Verfügung.

RDS Protection für ein einzelnes Konto konfigurieren

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich RDS Protection.
3. Auf der Seite RDS Protection wird der aktuelle Status Ihres Kontos angezeigt. Sie können das Feature jederzeit aktivieren oder deaktivieren, indem Sie Aktivieren oder Deaktivieren auswählen. Bestätigen Sie Ihre Auswahl.

API/CLI

Führen Sie den API-Vorgang updateDetector aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen `name` als `RDS_LOGIN_EVENTS` und `status` als `ENABLED` oder `DISABLED` übergeben.

Sie können den RDS-Schutz auch aktivieren oder deaktivieren, indem Sie den folgenden AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie Ihre eigene gültige *`Detektor-ID`* verwenden.

> **Note**
>
> Der folgende Beispielcode aktiviert RDS Protection. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "RDS_LOGIN_EVENTS", "Status" : "ENABLED"}]'
```

Konfiguration von RDS Protection in Umgebungen mit mehreren Konten

In einer Umgebung mit mehreren Konten hat nur das delegierte GuardDuty Administratorkonto die Möglichkeit, die RDS-Schutzfunktion für die Mitgliedskonten in der Organisation zu aktivieren oder zu deaktivieren. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Dieses delegierte GuardDuty Administratorkonto kann festlegen, dass die Überwachung der RDS-Anmeldeaktivitäten für alle neuen Konten automatisch aktiviert wird, wenn sie der Organisation beitreten. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten bei Amazon. GuardDuty

Konfiguration des RDS-Schutzes für ein delegiertes Administratorkonto GuardDuty

Wählen Sie Ihre bevorzugte Zugriffsmethode, um RDS Login Activity Monitoring für das delegierte GuardDuty Administratorkonto zu konfigurieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen des Verwaltungskontos verwenden.
2. Wählen Sie im Navigationsbereich RDS Protection.
3. Wählen Sie auf der Seite RDS Protection die Option Bearbeiten.
4. Führen Sie eine der folgenden Aktionen aus:

   Verwendung von Für alle Konten aktivieren

   - Wählen Sie Für alle Konten aktivieren. Dadurch wird der Schutzplan für alle aktiven GuardDuty Konten in Ihrer AWS Organisation aktiviert, einschließlich der neuen Konten, die der Organisation beitreten.
   - Wählen Sie Speichern.

   Verwendung von Konten manuell konfigurieren

   - Um den Schutzplan nur für das delegierte GuardDuty Administratorkonto zu aktivieren, wählen Sie Konten manuell konfigurieren.

- Wählen Sie im Abschnitt für das delegierte GuardDuty Administratorkonto (dieses Konto) die Option Aktivieren aus.
- Wählen Sie Speichern.

API/CLI

Führen Sie den API-Vorgang updateDetector aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen `name` als `RDS_LOGIN_EVENTS` und `status` als `ENABLED` oder `DISABLED` übergeben.

Sie können den RDS-Schutz aktivieren oder deaktivieren, indem Sie den folgenden AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie die gültige *`Melder-ID`* des delegierten GuardDuty Administratorkontos verwenden.

> **Note**
>
> Der folgende Beispielcode aktiviert RDS Protection. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Die `detectorId` für Ihr Konto und Ihre aktuelle Region gültige Adresse finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 555555555555 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

Automatische Aktivierung von RDS Protection für alle Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um das Feature RDS Protection für alle Mitgliedskonten zu aktivieren. Dazu gehören der delegierte Administrator, bestehende Mitgliedskonten und die neuen Konten, die der Organisation beitreten.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.

2. Führen Sie eine der folgenden Aktionen aus:

   Verwenden der Seite RDS Protection

   1. Wählen Sie im Navigationsbereich RDS Protection.
   2. Wählen Sie Für alle Konten aktivieren. Diese Aktion aktiviert automatisch RDS Protection sowohl für bestehende als auch für neue Konten in der Organisation.
   3. Wählen Sie Speichern.

   > **Note**
   >
   > Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

   Verwenden der Seite Konten

   1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
   2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren und anschließend Konten auf Einladung hinzufügen.
   3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter RDS Login Activity Monitoring die Option Für alle Konten aktivieren.
   4. Wählen Sie Speichern.

   Falls Sie die Option Für alle Konten aktivieren nicht verwenden können, finden Sie weitere Informationen unter Selektives Aktivieren oder Deaktivieren von RDS Protection für Mitgliedskonten.

API/CLI

- Um RDS Protection für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen *`Detektor-ID`* auf.

- Das folgende Beispiel zeigt, wie Sie RDS Protection für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

RDS Protection für alle vorhandenen aktiven Mitgliedskonten aktivieren

Wählen Sie Ihre bevorzugte Zugriffsmethode, um RDS Protection für alle vorhandenen aktiven Mitgliedskonten in Ihrer Organisation zu aktivieren.

Console

RDS Protection für alle vorhandenen aktiven Mitgliedskonten konfigurieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldeinformationen für das delegierte GuardDuty Administratorkonto an.

2. Wählen Sie im Navigationsbereich RDS Protection.
3. Auf der Seite RDS Protection können Sie den aktuellen Status der Konfiguration anzeigen. Wählen Sie im Abschnitt Aktive Mitgliedskonten die Option Aktionen.

4. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
5. Wählen Sie Bestätigen aus.

API/CLI

- Um RDS Protection für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen *`Detektor-ID`* auf.
- Das folgende Beispiel zeigt, wie Sie RDS Protection für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Automatische Aktivierung von RDS Protection für neue Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um RDS Protection für neue Konten, die Ihrer Organisation beitreten, zu aktivieren.

Console

Das delegierte GuardDuty Administratorkonto kann über die Konsole entweder über die Seite RDS-Schutz oder Konten neue Mitgliedskonten in einer Organisation aktivieren.

So aktivieren Sie RDS Protection für neue Mitgliedskonten automatisch

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.

2. Führen Sie eine der folgenden Aktionen aus:

   - Verwendung der Seite RDS Protection:

     1. Wählen Sie im Navigationsbereich RDS Protection.
     2. Wählen Sie auf der Seite RDS Protection die Option Bearbeiten.
     3. Wählen Sie Konten manuell konfigurieren.
     4. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Dieser Schritt stellt sicher, dass bei jedem Beitritt eines neuen Kontos zu Ihrer Organisation RDS Protection automatisch für das Konto aktiviert wird. Nur das delegierte GuardDuty Administratorkonto der Organisation kann diese Konfiguration ändern.
     5. Wählen Sie Speichern.

   - Verwenden der Seite Konten:

     1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
     2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren.
     3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter RDS Login Activity Monitoring die Option Für neue Konten aktivieren.
     4. Wählen Sie Speichern.

API/CLI

- Um RDS Protection für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den API-Vorgang UpdateOrganizationConfiguration mit Ihrer eigenen *`Detektor-ID`* auf.
- Das folgende Beispiel zeigt, wie Sie RDS Protection für ein einzelnes Mitgliedskonto aktivieren können. Informationen zur Deaktivierung finden Sie unter Selektives Aktivieren oder Deaktivieren von RDS Protection für Mitgliedskonten. Wenn Sie es nicht für alle neuen Konten aktivieren möchten, die der Organisation beitreten, legen Sie die Einstellung `autoEnable` auf `NONE` fest.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "RDS_LOGIN_EVENTS", "AutoEnable": "NEW"}]'
```

> **Note**
>
> Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Selektives Aktivieren oder Deaktivieren von RDS Protection für Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die Überwachung von RDS-Anmeldeaktivitäten für bestimmte Mitgliedskonten zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.

2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.

   Auf der Seite Konten finden Sie in der Spalte RDS-Anmeldeaktivität den Status Ihres Mitgliedskontos.

3. So können Sie die RDS-Anmeldeaktivität selektiv aktivieren oder deaktivieren

   Wählen Sie das Konto aus, für das Sie RDS Protection konfigurieren möchten. Sie können mehrere Konten gleichzeitig auswählen. Wählen Sie im Dropdown-Menü Schutzpläne bearbeiten die Option RDS-Anmeldeaktivität und dann die entsprechende Option aus.

API/CLI

Um RDS Protection für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen *Detektor-ID* auf.

Das folgende Beispiel zeigt, wie Sie RDS Protection für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

> **Note**
>
> Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Feature in RDS Protection

Überwachung der RDS-Anmeldeaktivitäten

Die RDS-Anmeldeaktivität erfasst sowohl erfolgreiche als auch fehlgeschlagene Anmeldeversuche zur Unterstützte Amazon-Aurora-Datenbanken in Ihrer AWS -Umgebung. Um Sie beim Schutz Ihrer Datenbanken zu unterstützen, überwacht GuardDuty RDS Protection kontinuierlich die Anmeldeaktivitäten im Hinblick auf potenziell verdächtige Anmeldeversuche. Beispielsweise könnte ein Angreifer versuchen, Brute-Force-Zugriff auf eine Amazon-Aurora-Datenbank zu erlangen, indem er das Passwort der Datenbank errät.

Wenn Sie die RDS-Schutzfunktion aktivieren, beginnt GuardDuty automatisch die Überwachung der RDS-Anmeldeaktivitäten für Ihre Datenbanken direkt vom Aurora-Service aus. Wenn es Hinweise auf

ein ungewöhnliches Anmeldeverhalten gibt, GuardDuty generiert dies einen Befund mit Einzelheiten über die potenziell gefährdete Datenbank. Wenn Sie RDS Protection zum ersten Mal aktivieren oder eine neu erstellte Datenbank-Instance haben, ist eine Lernphase erforderlich, um das normale Verhalten als Grundlage zu nehmen. Aus diesem Grund kann es sein, dass neu aktivierte oder neu erstellte Datenbank-Instances bis zu zwei Wochen lang keine anomalen Anmelde-Erkenntnisse aufweisen.

Die RDS-Schutzfunktion erfordert keine zusätzliche Einrichtung. Sie hat keine Auswirkungen auf Ihre bestehenden Amazon Aurora Aurora-Datenbankkonfigurationen. GuardDuty verwaltet Ihre unterstützten Datenbanken oder RDS-Anmeldeaktivitäten nicht und stellt Ihnen die RDS-Anmeldeaktivität auch nicht zur Verfügung.

Wenn Sie sich dafür entscheiden, die RDS-Schutzfunktion für neue Mitgliedskonten automatisch zu aktivieren, wenn diese Ihrer Organisation beitreten, wird diese Aktion automatisch GuardDuty für diese neuen Mitgliedskonten aktiviert. Weitere Informationen zur Konfiguration der Überwachung der RDS-Anmeldeaktivitäten als Feature finden Sie unter GuardDuty RDS-Schutz.

GuardDuty Überwachung der Laufzeit

Runtime Monitoring beobachtet und analysiert Ereignisse auf Betriebssystemebene, Netzwerk- und Dateiereignisse, um Ihnen zu helfen, potenzielle Bedrohungen in bestimmten AWS Workloads in Ihrer Umgebung zu erkennen.

GuardDuty hat Runtime Monitoring ursprünglich veröffentlicht, um nur Amazon Elastic Kubernetes Service (Amazon EKS) -Ressourcen zu unterstützen. Jetzt können Sie jedoch auch die Runtime Monitoring-Funktion verwenden, um Bedrohungen für Ihre AWS Fargate Amazon Elastic Container Service- (Amazon ECS) - und Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen zu erkennen.

In diesem Dokument und anderen Abschnitten, die sich auf Runtime Monitoring beziehen, GuardDuty verwendet die Terminologie des Ressourcentyps, um sich auf Amazon EKS-, Fargate, Amazon ECS- und Amazon EC2 EC2-Ressourcen zu beziehen.

Runtime Monitoring verwendet einen GuardDuty Security Agent, der Einblicke in das Laufzeitverhalten wie Dateizugriff, Prozessausführung, Befehlszeilenargumente und Netzwerkverbindungen bietet. Für jeden Ressourcentyp, den Sie auf potenzielle Bedrohungen überwachen möchten, können Sie den Security Agent für diesen spezifischen Ressourcentyp entweder automatisch oder manuell verwalten (mit Ausnahme von Fargate (nur Amazon ECS)). Wenn Sie den Security Agent automatisch verwalten, erlauben Sie, GuardDuty den Security Agent in Ihrem Namen zu installieren und zu aktualisieren. Wenn Sie den Security Agent für Ihre Ressourcen jedoch manuell verwalten, sind Sie dafür verantwortlich, den Security Agent bei Bedarf zu installieren und zu aktualisieren.

Mit dieser erweiterten Funktion GuardDuty können Sie potenzielle Bedrohungen identifizieren und darauf reagieren, die möglicherweise auf Anwendungen und Daten abzielen, die in Ihren individuellen Workloads und Instanzen ausgeführt werden. Beispielsweise kann eine Bedrohung potenziell damit beginnen, dass ein einzelner Container kompromittiert wird, auf dem eine anfällige Webanwendung ausgeführt wird. Diese Webanwendung verfügt möglicherweise über Zugriffsberechtigungen für die zugrunde liegenden Container und Workloads. In diesem Szenario könnten falsch konfigurierte Anmeldeinformationen möglicherweise zu einem umfassenderen Zugriff auf das Konto und die darin gespeicherten Daten führen.

Durch die Analyse der Laufzeitereignisse der einzelnen Container und Workloads GuardDuty kann in einer Anfangsphase potenziell eine Kompromittierung eines Containers und der zugehörigen

AWS Anmeldeinformationen erkannt und Versuche, Berechtigungen zu erweitern, verdächtige API-Anfragen und böswillige Zugriffe auf die Daten in Ihrer Umgebung erkannt werden.

Inhalt

Funktionsweise

Um Runtime Monitoring verwenden zu können, müssen Sie Runtime Monitoring aktivieren und anschließend den GuardDuty Security Agent verwalten. In der folgenden Liste wird dieser zweistufige Prozess erklärt:

1. Aktivieren Sie Runtime Monitoring für Ihr Konto, damit es die Runtime-Ereignisse akzeptieren GuardDuty kann, die es von Ihren Amazon EC2 EC2-Instances, Amazon ECS-Clustern und Amazon EKS-Workloads empfängt.
2. Managen Sie den GuardDuty Agenten für die einzelnen Ressourcen, für die Sie das Laufzeitverhalten überwachen möchten. Je nach Ressourcentyp können Sie wählen, ob Sie den GuardDuty Security Agent entweder manuell installieren oder ihn in Ihrem Namen verwalten lassen GuardDuty möchten. Dies wird als automatische Agentenkonfiguration bezeichnet.

   GuardDuty verwendet Instanzidentitätsrollen, die den Security Agent für jeden Ressourcentyp authentifizieren, um die zugehörigen Laufzeitereignisse an den VPC-Endpunkt zu senden.

> **Note**
>
> GuardDuty macht die Runtime-Ereignisse für Sie nicht zugänglich.

Wenn Sie den Security Agent (entweder manuell oder über GuardDuty) in EKS Runtime Monitoring oder Runtime Monitoring for EC2-Instances verwalten und derzeit auf einer Amazon EC2 EC2-Instance bereitgestellt GuardDuty ist und diese Gesammelte Laufzeit-Ereignistypen von dieser Instance empfängt, GuardDuty wird Ihnen die Analyse der VPC-Flow-Logs von dieser Amazon EC2 EC2-Instance nicht in Rechnung gestellt. AWS-Konto Dies trägt dazu bei, doppelte Nutzungskosten für das Konto GuardDuty zu vermeiden.

In den folgenden Themen wird erklärt, wie die Aktivierung von Runtime Monitoring und die Verwaltung des GuardDuty Security Agents für jeden Ressourcentyp unterschiedlich funktionieren.

Inhalt

So funktioniert Runtime Monitoring mit Amazon EC2 EC2-Instances

Ihre Amazon EC2 EC2-Instances können mehrere Arten von Anwendungen und Workloads in Ihrer AWS Umgebung ausführen. Wenn Sie Runtime Monitoring aktivieren und den GuardDuty Security Agent verwalten, GuardDuty hilft er Ihnen, Bedrohungen in Ihren bestehenden Amazon EC2 EC2-Instances und potenziell neuen zu erkennen. Diese Funktion unterstützt auch von Amazon ECS verwaltete Amazon EC2 EC2-Instances.

Durch die Aktivierung von Runtime Monitoring können Runtime-Ereignisse von aktuell laufenden und neuen Prozessen innerhalb von Amazon EC2 EC2-Instances verarbeitet werden. GuardDuty GuardDuty erfordert einen Security Agent, an den Runtime-Ereignisse von Ihrer EC2-Instance gesendet werden. GuardDuty

Bei Amazon EC2 EC2-Instances arbeitet der GuardDuty Security Agent auf Instance-Ebene. Sie können entscheiden, ob Sie alle oder nur ausgewählte Amazon EC2 EC2-Instances in Ihrem Konto

überwachen möchten. Wenn Sie ausgewählte Instances verwalten möchten, ist der Security Agent nur für diese Instances erforderlich.

GuardDuty kann auch Laufzeitereignisse von neuen Aufgaben und bestehenden Aufgaben verarbeiten, die in Amazon EC2 EC2-Instances innerhalb von Amazon ECS-Clustern ausgeführt werden.

Um den GuardDuty Security Agent zu installieren, bietet Runtime Monitoring die folgenden zwei Optionen:

- Verwenden Sie die automatische Agentenkonfiguration (empfohlen), oder
- Den Security Agent manuell verwalten

Verwenden Sie die automatische Agentenkonfiguration über GuardDuty (empfohlen)

Verwenden Sie die automatische Agentenkonfiguration, die es GuardDuty ermöglicht, den Security Agent in Ihrem Namen auf Ihren Amazon EC2 EC2-Instances zu installieren. GuardDuty verwaltet auch die Updates für den Security Agent.

GuardDuty Installiert den Security Agent standardmäßig auf allen Instanzen in Ihrem Konto. Wenn Sie den Security Agent nur für ausgewählte EC2-Instances installieren und verwalten möchten GuardDuty , fügen Sie Ihren EC2-Instances nach Bedarf Inklusions- oder Ausschluss-Tags hinzu.

Manchmal möchten Sie möglicherweise nicht die Laufzeitereignisse für alle Amazon EC2 EC2-Instances überwachen, die zu Ihrem Konto gehören. In Fällen, in denen Sie die Runtime-Ereignisse für eine begrenzte Anzahl von Instances überwachen möchten, fügen Sie diesen ausgewählten Instances ein Inclusion-Tag wie`GuardDutyManaged`: `true` hinzu. Beginnend mit der Verfügbarkeit der automatisierten Agentenkonfiguration für Amazon EC2 gilt: Wenn Ihre EC2-Instance über ein Inclusion-Tag (`GuardDutyManaged`:`true`) verfügt, GuardDuty berücksichtigt das Tag und verwaltet den Security Agent für die ausgewählten Instances, auch wenn Sie die automatische Agentenkonfiguration nicht explizit aktivieren.

Wenn es jedoch eine begrenzte Anzahl von EC2-Instances gibt, für die Sie Laufzeitereignisse nicht überwachen möchten, fügen Sie diesen ausgewählten Instances ein Ausschluss-Tag (`GuardDutyManaged`:`false`) hinzu. GuardDuty berücksichtigt das Ausschluss-Tag, indem der Security Agent für diese EC2-Ressourcen weder installiert noch verwaltet wird.

Auswirkung

Wenn Sie die automatische Agentenkonfiguration in einer AWS-Konto oder einer Organisation verwenden, GuardDuty erlauben Sie, die folgenden Schritte in Ihrem Namen durchzuführen:

- GuardDuty erstellt eine SSM-Zuordnung für all Ihre Amazon EC2 EC2-Instances, die SSM-verwaltet werden und unter Fleet Manager in der https://console.aws.amazon.com/systems-manager/ -Konsole angezeigt werden.
- Verwendung von Inclusion-Tags bei deaktivierter automatisierter Agentenkonfiguration — Wenn Sie nach der Aktivierung von Runtime Monitoring die automatische Agentenkonfiguration nicht aktivieren, sondern Ihrer Amazon EC2 EC2-Instance ein Inclusion-Tag hinzufügen, bedeutet dies, dass Sie erlauben, den Security Agent in Ihrem Namen GuardDuty zu verwalten. Die SSM-Zuordnung installiert dann den Security Agent in jeder Instance, die über das Inklusion-Tag (:) `GuardDutyManaged` verfügt. `true`
- Wenn Sie die automatische Agentenkonfiguration aktivieren, installiert die SSM-Zuordnung den Security Agent dann auf allen EC2-Instances, die zu Ihrem Konto gehören.
- Verwenden von Ausschluss-Tags mit automatisierter Agentenkonfiguration — Bevor Sie die automatische Agentenkonfiguration aktivieren und Ihrer Amazon EC2 EC2-Instance ein Ausschluss-Tag hinzufügen, bedeutet dies, dass Sie die Installation und Verwaltung des Security Agents für diese ausgewählte Instance verhindern. GuardDuty

  Wenn Sie nun die automatische Agentenkonfiguration aktivieren, installiert und verwaltet die SSM-Verbindung den Security Agent in allen EC2-Instances mit Ausnahme der Instances, die mit dem Exclusion-Tag gekennzeichnet sind.
- GuardDuty erstellt VPC-Endpoints in allen VPCs, einschließlich gemeinsam genutzter VPCs, sofern in dieser VPC mindestens eine Linux EC2-Instance vorhanden ist, die sich nicht im Status Beendet oder Herunterfahren der Instance befindet. Informationen zu den verschiedenen Instance-Status finden Sie unter Instance-Lebenszyklus im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

  GuardDuty unterstützt Verwenden einer gemeinsam genutzten VPC mit automatisierten Sicherheitsagenten auch. Wenn alle Voraussetzungen für Ihre Organisation erfüllt sind AWS-Konto, GuardDuty wird die gemeinsam genutzte VPC zum Empfangen von Laufzeitereignissen verwendet.

> **Note**
>
> Für die Nutzung der erstellten VPC-Endpoints fallen keine zusätzlichen Kosten an GuardDuty .

Den Security Agent manuell verwalten

Es gibt zwei Möglichkeiten, den Security Agent für Amazon EC2 manuell zu verwalten:

- Verwenden Sie GuardDuty verwaltete Dokumente AWS Systems Manager , um den Security Agent auf Ihren Amazon EC2 EC2-Instances zu installieren, die bereits über SSM verwaltet werden.

  Wenn Sie eine neue Amazon EC2 EC2-Instance starten, stellen Sie sicher, dass sie SSM-aktiviert ist.
- Verwenden Sie RPM Package Manager (RPM) -Skripts, um den Security Agent auf Ihren Amazon EC2 EC2-Instances zu installieren, unabhängig davon, ob sie SSM-verwaltet werden oder nicht.

Nächster Schritt

Erste Schritte mit der Runtime Monitoring-Konfiguration zur Überwachung Ihrer Amazon EC2 EC2-Instances finden Sie unterVoraussetzungen für die Unterstützung von Amazon EC2 EC2-Instances.

So funktioniert Runtime Monitoring mit Fargate (nur Amazon ECS)

Wenn Sie Runtime Monitoring aktivieren, ist GuardDuty es bereit, die Laufzeitereignisse einer Aufgabe zu verarbeiten. Diese Aufgaben werden innerhalb der Amazon ECS-Cluster ausgeführt, die wiederum auf den AWS Fargate (Fargate) Instances ausgeführt werden. GuardDuty Um diese Runtime-Ereignisse empfangen zu können, müssen Sie den vollständig verwalteten, dedizierten Security Agent verwenden.

Derzeit unterstützt Runtime Monitoring die von gestarteten Aufgaben nicht. AWS CodePipeline

Derzeit unterstützt Runtime Monitoring die Verwaltung des Security Agents für Ihre Amazon ECS-Cluster (AWS Fargate) nur über GuardDuty. Die manuelle Verwaltung des Security Agents auf Amazon ECS-Clustern wird nicht unterstützt.

Sie können zulassen GuardDuty , dass der GuardDuty Security Agent in Ihrem Namen verwaltet wird, indem Sie die automatische Agentenkonfiguration für ein AWS Konto oder eine Organisation

verwenden. GuardDuty beginnt mit der Bereitstellung des Security Agents für die neuen Fargate-Aufgaben, die in Ihren Amazon ECS-Clustern gestartet werden. In der folgenden Liste wird angegeben, was zu erwarten ist, wenn Sie den GuardDuty Security Agent aktivieren.

Auswirkungen der Aktivierung des GuardDuty Security Agents

GuardDuty erstellt einen Virtual Private Cloud (VPC) -Endpunkt

Wenn Sie den GuardDuty Security Agent bereitstellen, GuardDuty erstellt er einen VPC-Endpunkt, über den der Security Agent die Runtime-Ereignisse übermittelt GuardDuty.

> **Note**
>
> Für die Nutzung der erstellten VPC-Endpoints fallen keine zusätzlichen Kosten an GuardDuty .

GuardDuty fügt einen Sidecar-Container hinzu

Bei einer neuen Fargate-Aufgabe oder einem neuen Fargate-Dienst, der gestartet wird, hängt sich ein GuardDuty Container (Sidecar) an jeden Container innerhalb der Amazon ECS Fargate-Aufgabe an. Der GuardDuty Security Agent wird innerhalb des angehängten Containers ausgeführt. GuardDuty Auf diese Weise GuardDuty können die Laufzeitereignisse jedes Containers erfasst werden, der im Rahmen dieser Tasks ausgeführt wird.

Wenn Sie eine Fargate-Aufgabe starten und der GuardDuty Container (Sidecar) nicht in einem fehlerfreien Zustand gestartet werden kann, ist Runtime Monitoring so konzipiert, dass die Ausführung der Aufgaben nicht verhindert wird.

Standardmäßig ist eine Fargate-Aufgabe unveränderlich. GuardDuty stellt den Sidecar nicht bereit, wenn sich eine Aufgabe bereits im laufenden Zustand befindet. Wenn Sie einen Container in einer bereits laufenden Aufgabe überwachen möchten, können Sie die Aufgabe beenden und erneut starten.

So funktioniert Runtime Monitoring mit Amazon EKS-Clustern

Runtime Monitoring verwendet ein EKS-Add-on `aws-guardduty-agent`, das auch als GuardDuty Security Agent bezeichnet wird. Nachdem der GuardDuty Security Agent auf Ihren EKS-Clustern installiert wurde, GuardDuty kann er Runtime-Ereignisse für diese EKS-Cluster empfangen.

Sie können die Laufzeitereignisse Ihrer Amazon EKS-Cluster entweder auf Konto- oder Clusterebene überwachen. Sie können den GuardDuty Security Agent nur für die Amazon EKS-Cluster verwalten, die Sie im Hinblick auf die Erkennung von Bedrohungen überwachen möchten. Sie können den GuardDuty Security Agent entweder manuell verwalten oder indem GuardDuty Sie die automatische Agentenkonfiguration verwenden, indem Sie die automatische Agentenkonfiguration verwenden.

Wenn Sie den Ansatz der automatisierten Agentenkonfiguration verwenden, GuardDuty um die Bereitstellung des Security Agents in Ihrem Namen zu verwalten, wird automatisch ein Amazon Virtual Private Cloud (Amazon VPC) -Endpunkt erstellt. Der Security Agent übermittelt die Runtime-Ereignisse über diesen Amazon VPC-Endpunkt an. GuardDuty

> **Note**
>
> Für die Nutzung der erstellten VPC-Endpoints fallen keine zusätzlichen Kosten an GuardDuty .

GuardDuty Unterstützt derzeit Amazon EKS-Cluster, die auf Amazon EC2 EC2-Instances ausgeführt werden. GuardDuty unterstützt keine Amazon EKS-Cluster, die auf laufen AWS Fargate.

Nach der Konfiguration von Runtime Monitoring

Beurteilen Sie die Runtime-Abdeckung

Nachdem Sie Runtime Monitoring aktiviert und den GuardDuty Security Agent installiert haben, empfehlen wir Ihnen, den Abdeckungsstatus der Ressource, auf der Sie den Security Agent installiert haben, kontinuierlich zu überprüfen. Der Deckungsstatus kann entweder Fehlerfrei oder Fehlerfrei sein. Der Deckungsstatus Fehlerfrei gibt an, dass GuardDuty die Laufzeitereignisse von der entsprechenden Ressource empfangen werden, wenn eine Aktivität auf Betriebssystemebene stattfindet.

Wenn der Abdeckungsstatus für die Ressource auf Fehlerfrei gesetzt GuardDuty wird, kann sie die Laufzeitereignisse empfangen und sie zur Bedrohungserkennung analysieren. Wenn eine potenzielle Sicherheitsbedrohung in den Aufgaben oder Anwendungen GuardDuty erkannt wird, die in Ihren Container-Workloads und -Instances ausgeführt werden, GuardDuty generiert das Programm einen oder mehrere Runtime Monitoring-Findetypen.

[1] Sie können Amazon EventBridge (EventBridge) auch so konfigurieren, dass Sie eine Benachrichtigung erhalten, wenn sich der Versicherungsstatus von Ungesund auf Gesund usw. ändert.

Weitere Informationen finden Sie unter Bewertung der Laufzeitabdeckung Ihrer Ressourcen.

GuardDuty erkennt potenzielle Bedrohungen

Sobald GuardDuty die Laufzeitereignisse für Ihre Ressource empfangen werden, beginnt es mit der Analyse dieser Ereignisse. Wenn eine potenzielle Sicherheitsbedrohung in einer Ihrer Amazon EC2 EC2-Instances, Amazon ECS-Cluster oder Amazon EKS-Cluster GuardDuty erkannt wird, generiert es eine oder mehrereRuntime Monitoring: Typen finden. Sie können auf die Ergebnisdetails zugreifen, um die betroffenen Ressourcen einzusehen.

Wie funktioniert die kostenlose 30-Tage-Testversion in Runtime Monitoring

Die 30-tägige kostenlose Testphase funktioniert unterschiedlich für neue GuardDuty Konten und für bestehende Konten, für die EKS Runtime Monitoring bereits aktiviert wurde, bevor die Runtime Monitoring-Funktion auf Amazon EC2 EC2-Instances ausgedehnt wurde und AWS Fargate (nur Amazon ECS).

Ich verwende die GuardDuty Testphase oder habe EKS Runtime Monitoring noch nie aktiviert

In der folgenden Liste wird erklärt, wie die kostenlose 30-Tage-Testphase funktioniert, wenn Sie entweder die GuardDuty 30-Tage-Testphase verwenden oder EKS Runtime Monitoring noch nie aktiviert haben:

- Wenn Sie Runtime Monitoring und EKS Runtime Monitoring GuardDuty zum ersten Mal aktivieren, werden Runtime Monitoring und EKS Runtime Monitoring standardmäßig nicht aktiviert.

  Wenn Sie Runtime Monitoring für Ihr Konto oder Ihre Organisation aktivieren, stellen Sie sicher, dass Sie auch den GuardDuty Security Agent für die Ressource konfigurieren, die Sie auf Bedrohungserkennung überwachen möchten. Wenn Sie beispielsweise Runtime Monitoring für Ihre Amazon EC2-Instances verwenden möchten, müssen Sie nach der Aktivierung von Runtime Monitoring auch den Security Agent für Amazon EC2 konfigurieren. Sie können wählen, ob Sie dies manuell oder automatisch über tun möchten. GuardDuty

- Der Runtime Monitoring-Schutzplan ist auf Kontoebene aktiviert. Die kostenlose 30-Tage-Testphase gilt auf Ressourcenebene. Nachdem der GuardDuty Security Agent für einen bestimmten Ressourcentyp bereitgestellt wurde, beginnt die kostenlose 30-Tage-Testversion, sobald GuardDuty das erste Runtime-Ereignis im Zusammenhang mit diesem Ressourcentyp eintrifft. Sie haben den GuardDuty Agenten beispielsweise auf Ressourcenebene bereitgestellt (für Amazon EC2 EC2-Instance, Amazon ECS-Cluster und Amazon EKS-Cluster). Wenn das GuardDuty erste Runtime-Event für eine Amazon EC2-Instance eingeht, startet die kostenlose 30-Tage-Testversion nur für Amazon EC2.
- Wenn Sie nur EKS Runtime Monitoring aktivieren möchten — Wenn Sie EKS Runtime Monitoring GuardDuty zum ersten Mal aktivieren, ist EKS Runtime Monitoring standardmäßig nicht aktiviert (nach der Veröffentlichung von Runtime Monitoring). Sie müssen EKS Runtime Monitoring aktivieren. Um ihn optimal zu nutzen, stellen Sie sicher, dass Sie den GuardDuty Security Agent entweder manuell verwalten oder die automatische Agentenkonfiguration aktivieren, sodass der Agent in Ihrem Namen GuardDuty verwaltet wird. Ihre 30-tägige kostenlose Testphase für EKS Runtime Monitoring beginnt, wenn GuardDuty das erste Runtime-Ereignis für die Amazon EKS-Ressource eingeht.

Ich habe EKS Runtime Monitoring vor dem Start von Runtime Monitoring aktiviert

- Für ein vorhandenes GuardDuty Konto, für das der EKS Runtime Monitoring-Schutzplan aktiviert ist und das die GuardDuty Konsolenerfahrung verwendet, um diesen Schutzplan zu verwenden — Mit der Ankündigung von Runtime Monitoring wurde das Erlebnis der EKS Runtime Monitoring-Konsole nun in Runtime Monitoring konsolidiert. Ihre bestehende Konfiguration für EKS Runtime Monitoring bleibt unverändert. Sie können die API/CLI-Unterstützung weiterhin verwenden, um Operationen im Zusammenhang mit EKS Runtime Monitoring auszuführen.
- Um EKS Runtime Monitoring als Teil von Runtime Monitoring verwenden zu können, müssen Sie Runtime Monitoring für Ihr Konto oder Ihre Organisation konfigurieren. Informationen zur Beibehaltung derselben Konfiguration für Runtime Monitoring finden Sie unterMigration von EKS Runtime Monitoring zu Runtime Monitoring. Dies hat jedoch keine Auswirkungen auf Ihre kostenlose 30-Tage-Testversion für die Amazon EKS-Ressource.
- Der Runtime Monitoring-Schutzplan ist auf Kontoebene pro Region aktiviert. Nachdem der GuardDuty Security Agent auf einem der angegebenen Ressourcentypen (Amazon EC2-Instance und Amazon ECS-Cluster) bereitgestellt wurde, beginnt die kostenlose 30-Tage-Testversion,

sobald das erste Runtime-Ereignis im Zusammenhang mit der Ressource GuardDuty empfangen wird. Für jeden Ressourcentyp ist eine kostenlose 30-Tage-Testversion verfügbar.

Nachdem Sie Runtime Monitoring aktiviert haben, entscheiden Sie sich beispielsweise dafür, den GuardDuty Agenten nur auf einer Amazon EC2 EC2-Instance bereitzustellen. Die kostenlose 30-Tage-Testversion für diese Ressource beginnt erst, wenn das erste Runtime-Ereignis für eine Amazon EC2 EC2-Instance GuardDuty empfangen wird. Später, wenn Sie den GuardDuty Agenten für Fargate bereitstellen (nur Amazon ECS), beginnt die kostenlose 30-Tage-Testversion für diese Ressource erst, wenn das erste Runtime-Ereignis für den Amazon ECS-Cluster GuardDuty empfangen wird. Da Sie EKS Runtime Monitoring bereits für Ihr Konto aktiviert haben, wird die kostenlose 30-Tage-Testversion für eine Amazon EKS-Ressource GuardDuty nicht zurückgesetzt.

Schlüsselkonzepte — Ansätze zur Verwaltung von GuardDuty Security Agents

Beachten Sie die wichtigsten Konzepte, die Ihnen bei der Verwaltung des Security Agents auf Ihren Amazon EKS-Clustern und Amazon ECS-Clustern helfen.

Inhalt

Fargate-Ressource (nur Amazon ECS) — Methoden zur Verwaltung von GuardDuty Sicherheitsagenten

Runtime Monitoring bietet Ihnen die Möglichkeit, potenzielle Sicherheitsbedrohungen entweder auf allen Amazon ECS-Clustern (Kontoebene) oder auf ausgewählten Clustern (Cluster-Ebene) in Ihrem Konto zu erkennen. Wenn Sie die automatische Agentenkonfiguration für jede auszuführende Amazon ECS Fargate-Aufgabe aktivieren, GuardDuty wird für jeden Container-Workload innerhalb dieser Aufgabe ein Sidecar-Container hinzugefügt. Der GuardDuty Security Agent wird in diesem Sidecar-Container bereitgestellt. Auf diese Weise GuardDuty erhalten Sie Einblick in das Laufzeitverhalten der Container in den Amazon ECS-Aufgaben.

Derzeit unterstützt Runtime Monitoring die Verwaltung des Security Agents für Ihre Amazon ECS-Cluster (AWS Fargate) nur über GuardDuty. Die manuelle Verwaltung des Security Agents auf Amazon ECS-Clustern wird nicht unterstützt.

Bevor Sie Ihre Konten konfigurieren, sollten Sie abwägen, wie Sie den GuardDuty Security Agent verwalten und möglicherweise das Laufzeitverhalten der Container überwachen möchten, die zu den Amazon ECS-Aufgaben gehören. Ziehen Sie die folgenden Ansätze in Betracht.

Themen

GuardDuty Sicherheitsagenten für alle Amazon ECS-Cluster verwalten

Dieser Ansatz hilft Ihnen dabei, potenzielle Sicherheitsbedrohungen auf Kontoebene zu erkennen. Verwenden Sie diesen Ansatz, wenn Sie potenzielle Sicherheitsbedrohungen für alle Amazon ECS-Cluster erkennen möchten GuardDuty , die zu Ihrem Konto gehören.

Den GuardDuty Sicherheitsagenten für die meisten Amazon ECS-Cluster verwalten, einige Amazon ECS-Cluster jedoch ausschließen

Verwenden Sie diesen Ansatz, wenn GuardDuty Sie potenzielle Sicherheitsbedrohungen für die meisten Amazon ECS-Cluster in Ihrer AWS Umgebung erkennen, einige Cluster jedoch ausschließen möchten. Dieser Ansatz hilft Ihnen, das Laufzeitverhalten der Container innerhalb Ihrer Amazon ECS-Aufgaben auf Cluster-Ebene zu überwachen. Die Anzahl der Amazon ECS-Cluster, die zu Ihrem Konto gehören, beträgt beispielsweise 1000. Sie möchten jedoch nur 930 Amazon ECS-Cluster überwachen.

Bei diesem Ansatz müssen Sie den Amazon ECS-Clustern, die Sie nicht überwachen möchten, ein vordefiniertes GuardDuty Tag hinzufügen. Weitere Informationen finden Sie unter Verwaltung eines automatisierten Sicherheitsagenten für Fargate (nur Amazon ECS).

GuardDuty Sicherheitsagenten für ausgewählte Amazon ECS-Cluster verwalten

Verwenden Sie diesen Ansatz, wenn GuardDuty Sie potenzielle Sicherheitsbedrohungen für einige der Amazon ECS-Cluster erkennen möchten. Dieser Ansatz hilft Ihnen, das Laufzeitverhalten der

Container innerhalb Ihrer Amazon ECS-Aufgaben auf Cluster-Ebene zu überwachen. Die Anzahl der Amazon ECS-Cluster, die zu Ihrem Konto gehören, beträgt beispielsweise 1000. Sie möchten jedoch nur 230 Cluster überwachen.

Bei diesem Ansatz müssen Sie den Amazon ECS-Clustern, die Sie überwachen möchten, ein vordefiniertes GuardDuty Tag hinzufügen. Weitere Informationen finden Sie unter Verwaltung eines automatisierten Sicherheitsagenten für Fargate (nur Amazon ECS).

Amazon EKS-Cluster — Ansätze zur Verwaltung von GuardDuty Security Agents

GuardDuty Um die Runtime-Ereignisse aus Ihren EKS-Clustern auf Konto- oder Clusterebene verarbeiten zu können, ist es erforderlich, den GuardDuty Security Agent für die entsprechenden Cluster zu verwalten.

Methoden zur Verwaltung des GuardDuty Security Agents

Vor dem 13. September 2023 konnten Sie den Security Agent so konfigurieren, GuardDuty dass er auf Kontoebene verwaltet wird. Dieses Verhalten deutete darauf hin, dass der Security Agent standardmäßig auf allen EKS-Clustern verwaltet GuardDuty wird, die zu einem gehören AWS-Konto. GuardDuty Bietet jetzt eine detaillierte Funktion, die Ihnen bei der Auswahl der EKS-Cluster hilft, auf denen Sie den Security Agent verwalten GuardDuty möchten.

Wenn Sie Den GuardDuty Security Agent manuell verwalten wählen, können Sie immer noch die EKS-Cluster auswählen, die Sie überwachen möchten. Um den Agenten jedoch manuell verwalten zu können, ist die Erstellung eines Amazon-VPC-Endpunkts für Ihr AWS-Konto eine Voraussetzung.

> **Note**
>
> Unabhängig davon, welchen Ansatz Sie zur Verwaltung des GuardDuty Security Agents verwenden, ist EKS Runtime Monitoring immer auf Kontoebene aktiviert.

Themen

- Verwalten Sie den Security Agent über GuardDuty
- Den GuardDuty Security Agent manuell verwalten

Verwalten Sie den Security Agent über GuardDuty

GuardDuty verteilt und verwaltet den Security Agent in Ihrem Namen. Sie können die EKS-Cluster in Ihrem Konto jederzeit überwachen, indem Sie einen der folgenden Ansätzen verwenden.

Themen

Alle EKS-Cluster überwachen

- Wann Sie diesen Ansatz verwenden sollten — Verwenden Sie diesen Ansatz, wenn Sie den Security Agent für alle EKS-Cluster in Ihrem Konto bereitstellen und verwalten möchten GuardDuty . Standardmäßig GuardDuty wird der Security Agent auch auf einem potenziell neuen EKS-Cluster installiert, der in Ihrem Konto erstellt wurde.
- Auswirkungen dieses Ansatzes:
  - GuardDuty erstellt einen Amazon Virtual Private Cloud (Amazon VPC) -Endpunkt, über den der GuardDuty Security Agent die Runtime-Ereignisse übermittelt GuardDuty. Es fallen keine zusätzlichen Kosten für die Erstellung des Amazon VPC-Endpunkts an, wenn Sie den Security Agent über GuardDuty verwalten.
  - Es ist erforderlich, dass Ihr Worker-Knoten über einen gültigen Netzwerkpfad zu einem aktiven `guardduty-data` VPC-Endpunkt verfügt. GuardDuty stellt den Security Agent auf Ihren EKS-Clustern bereit. Amazon Elastic Kubernetes Service (Amazon EKS) koordiniert die Bereitstellung des Sicherheitsagenten auf den Knoten innerhalb der EKS-Cluster.
  - GuardDuty Wählt auf der Grundlage der IP-Verfügbarkeit das Subnetz aus, um einen VPC-Endpunkt zu erstellen. Wenn Sie erweiterte Netzwerktopologien verwenden, müssen Sie überprüfen, ob die Konnektivität möglich ist.
- Überlegung – Wenn Sie diese Option verwenden, erstellt die EKS-Laufzeit-Überwachung derzeit keine gemeinsam genutzte VPC.

Alle EKS-Cluster überwachen und ausgewählte EKS-Cluster ausschließen

- Wann Sie diesen Ansatz verwenden sollten — Verwenden Sie diesen Ansatz, wenn Sie den Security Agent für alle EKS-Cluster in Ihrem Konto verwalten, aber ausgewählte EKS-Cluster

ausschließen möchten GuardDuty . Bei dieser Methode wird ein Tag-basierter [1] Ansatz verwendet, bei dem Sie die EKS-Cluster taggen können, für die Sie keine Laufzeit-Ereignisse erhalten möchten. Das vordefinierte Tag muss `GuardDutyManaged-false` als Schlüssel-Wert-Paar haben.

- Auswirkungen dieses Ansatzes:
  - Bei diesem Ansatz müssen Sie die automatische GuardDuty Agentenverwaltung erst aktivieren, nachdem Sie den EKS-Clustern, die Sie von der Überwachung ausschließen möchten, Tags hinzugefügt haben.

    Daher gilt auch für diesen Ansatz die Auswirkung von Verwalten Sie den Security Agent über GuardDuty. Wenn Sie Tags hinzufügen, bevor Sie die automatische GuardDuty Agentenverwaltung aktivieren, GuardDuty wird der Security Agent für die EKS-Cluster, die von der Überwachung ausgeschlossen sind, weder bereitgestellt noch verwaltet.
- Überlegungen:
  - Sie müssen das Tag-Schlüssel-Wert-Paar wie folgt hinzufügen`GuardDutyManaged`: `false` für die ausgewählten EKS-Cluster, bevor Sie die automatische Agentenkonfiguration aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern installiert, bis Sie das Tag verwenden.
  - Sie müssen verhindern, dass die Tags geändert werden, es sei denn, es handelt sich um vertrauenswürdige Identitäten.

    > **Important**
    >
    > Verwalten Sie die Berechtigungen zum Ändern des Werts des `GuardDutyManaged`-Tags für Ihren EKS-Cluster mithilfe von Service-Kontrollrichtlinie oder IAM-Richtlinien. Weitere Informationen finden Sie unter Service Control Policies (SCPs) im AWS Organizations Benutzerhandbuch oder Control access to AWS resources im IAM-Benutzerhandbuch.
  - Bei einem potenziell neuen EKS-Cluster, den Sie nicht überwachen möchten, stellen Sie sicher, dass Sie bei der Erstellung dieses EKS-Clusters das Schlüssel-Wert-Paar `GuardDutyManaged-false` hinzufügen.
  - Bei diesem Ansatz werden auch dieselben Überlegungen berücksichtigt, wie für Alle EKS-Cluster überwachen angegeben.

Ausgewählte EKS-Cluster überwachen

- Wann Sie diesen Ansatz verwenden sollten — Verwenden Sie diesen Ansatz, wenn Sie GuardDuty die Updates für den Security Agent nur für ausgewählte EKS-Cluster in Ihrem Konto bereitstellen und verwalten möchten. Bei dieser Methode wird ein Tag-basierter [1]-Ansatz verwendet, bei dem Sie die EKS-Cluster markieren können, für die Sie Laufzeit-Ereignisse erhalten möchten.
- Auswirkungen dieses Ansatzes:
  - Durch die Verwendung von Inklusion-Tags GuardDuty wird der Security Agent automatisch nur für die ausgewählten EKS-Cluster bereitgestellt und verwaltet, die mit `GuardDutyManaged - true` als Schlüssel-Wert-Paar gekennzeichnet sind.
  - Dieser Ansatz hat auch die gleichen Auswirkungen, wie für Alle EKS-Cluster überwachen angegeben.
- Überlegungen:
  - Wenn der Wert des `GuardDutyManaged`-Tags nicht auf `true` festgelegt ist, funktioniert das Einschließen-Tag nicht wie erwartet, und dies kann sich auf die Überwachung Ihres EKS-Clusters auswirken.
  - Um sicherzustellen, dass Ihre ausgewählten EKS-Cluster überwacht werden, müssen Sie verhindern, dass die Tags geändert werden, es sei denn, es handelt sich um vertrauenswürdige Identitäten.

    > **Important**
    >
    > Verwalten Sie die Berechtigungen zum Ändern des Werts des `GuardDutyManaged`-Tags für Ihren EKS-Cluster mithilfe von Service-Kontrollrichtlinie oder IAM-Richtlinien. Weitere Informationen finden Sie unter Service Control Policies (SCPs) im AWS Organizations Benutzerhandbuch oder Control access to AWS resources im IAM-Benutzerhandbuch.

  - Bei einem potenziell neuen EKS-Cluster, den Sie nicht überwachen möchten, stellen Sie sicher, dass Sie bei der Erstellung dieses EKS-Clusters das Schlüssel-Wert-Paar `GuardDutyManaged-false` hinzufügen.
  - Bei diesem Ansatz werden auch dieselben Überlegungen berücksichtigt, wie für Alle EKS-Cluster überwachen angegeben.

[1]Weitere Informationen zum Markieren von ausgewählten EKS-Clustern finden Sie unter Markieren Ihrer Amazon-EKS-Ressourcen im Amazon-EKS-Benutzerhandbuch.

Den GuardDuty Security Agent manuell verwalten

- Wann sollten Sie diesen Ansatz verwenden — Verwenden Sie diesen Ansatz, wenn Sie den GuardDuty Security Agent auf all Ihren EKS-Clustern manuell verteilen und verwalten möchten. Stellen Sie sicher, dass EKS-Laufzeit-Überwachung für Ihre Konten aktiviert ist. Der GuardDuty Security Agent funktioniert möglicherweise nicht wie erwartet, wenn Sie EKS Runtime Monitoring nicht aktivieren.
- Auswirkung dieses Ansatzes — Sie müssen die Bereitstellung der GuardDuty Security Agent-Software in Ihren EKS-Clustern für alle Konten und für alle Standorte, AWS-Regionen an denen diese Funktion verfügbar ist, koordinieren.
- Überlegungen – Sie müssen einen sicheren Datenfluss unterstützen und gleichzeitig Sicherheitslücken im Auge behalten und diese schließen, da ständig neue Cluster und Workloads bereitgestellt werden.

GuardDuty Runtime Monitoring aktivieren

Bevor Sie Runtime Monitoring in Ihrem Konto aktivieren, stellen Sie sicher, dass der Ressourcentyp, für den Sie die Laufzeitereignisse überwachen möchten, die Plattformanforderungen unterstützt. Weitere Informationen finden Sie unter Voraussetzungen.

Wenn Sie EKS Runtime Monitoring vor dem Start von Runtime Monitoring verwendet haben, können Sie die APIs verwenden, um die bestehende Konfiguration für EKS Runtime Monitoring zu überprüfen und zu aktualisieren. Sie können Ihre bestehende Konfiguration auch von EKS Runtime Monitoring zu Runtime Monitoring migrieren. Weitere Informationen finden Sie unter Migration von EKS Runtime Monitoring zu Runtime Monitoring.

> **Note**
>
> Derzeit enthält diese Dokumentation Schritte zur Aktivierung von Runtime Monitoring für Ihre Konten und Ihr Unternehmen nur über die Konsole. Sie können Runtime Monitoring auch mithilfe von API-Aktionen oder AWS CLI für GuardDuty aktivieren.

Sie können Runtime Monitoring mithilfe der Schritte in den folgenden Themen konfigurieren.

Inhalt

Voraussetzungen für die Aktivierung von Runtime Monitoring

Um Runtime Monitoring zu aktivieren und den GuardDuty Security Agent zu verwalten, müssen Sie die Voraussetzungen für jeden Ressourcentyp erfüllen, den Sie auf Bedrohungserkennung überwachen möchten.

Inhalt

Voraussetzungen für die Unterstützung von Amazon EC2 EC2-Instances

Machen Sie EC2-Instanzen SSM-verwaltet

Die Amazon EC2 EC2-Instances, für die Sie Laufzeitereignisse überwachen GuardDuty möchten, müssen AWS Systems Manager (SSM) verwaltet werden. Dies gilt unabhängig davon, ob Sie GuardDuty den Security Agent automatisch oder manuell verwalten (außerMethode 2 — Mithilfe von RPM-Installationsskripten).

Informationen zur Verwaltung Ihrer Amazon EC2 EC2-Instances mit AWS Systems Manager finden Sie unter Systems Manager für Amazon EC2 EC2-Instances einrichten im AWS Systems Manager Benutzerhandbuch.

Validierung der architektonischen Anforderungen

Die Architektur Ihrer Betriebssystemdistribution kann sich auf das Verhalten des GuardDuty Security Agents auswirken. Sie müssen die folgenden Anforderungen erfüllen, bevor Sie Runtime Monitoring für Amazon EC2 EC2-Instances verwenden können:

- Derzeit ist die Runtime Monitoring-Unterstützung für Amazon EC2 nur für Linux-Versionen verfügbar. Obwohl die Unterstützung für Ubuntu derzeit nicht verfügbar ist, wird sie in naher future verfügbar sein. Abonnieren Sie den RSS-Feed, um Benachrichtigungen über Updates auf dieser Seite zu erhalten.

  Die folgende Tabelle zeigt die Betriebssystemdistribution, für die verifiziert wurde, dass sie den GuardDuty Security Agent für Amazon EC2 EC2-Instances unterstützt.

Betriebssystem-Verteilung	Kernel-Version	Kernel-Unterstützung	CPU-Architektur	
			x64 (AMD64)	Graviton (ARM64)
AL2 und AL2023	5.4, 5,10, 5,15, 6,1 * -	eBPF, Tracepoints, Kprobe	Unterstützt	Unterstützt

- Zusätzliche Anforderungen — Nur wenn Sie Amazon ECS/Amazon EC2 haben

  Für Amazon ECS/Amazon EC2 empfehlen wir, die neuesten Amazon ECS-optimierten AMIs (vom 29. September 2023 oder später) oder Amazon ECS Agent Version v1.77.0 zu verwenden.

- *Derzeit können mit der Kernel-Version `6.1` keine Dateien generiert werden, die sich auf Folgendes beziehen. GuardDuty Runtime Monitoring: Typen finden DNS-Ereignisse

Überprüfung der Service-Control-Richtlinie Ihrer Organisation

Wenn Sie eine Service Control Policy (SCP) zur Verwaltung von Berechtigungen in Ihrer Organisation eingerichtet haben, stellen Sie sicher, dass die Richtlinie die Erlaubnis nicht verweigert. `guardduty:SendSecurityTelemetry` Sie ist erforderlich GuardDuty , um Runtime Monitoring für verschiedene Ressourcentypen zu unterstützen.

Wenn Sie ein Mitgliedskonto sind, stellen Sie eine Verbindung mit dem zugehörigen delegierten Administrator her. Informationen zur Verwaltung von SCPs für Ihre Organisation finden Sie unter Service Control Policies (SCPs).

Bei Verwendung der automatisierten Agentenkonfiguration

Dazu Verwenden Sie die automatische Agentenkonfiguration (empfohlen) AWS-Konto müssen Sie die folgenden Voraussetzungen erfüllen:

- Wenn Sie Inclusion-Tags mit automatisierter Agentenkonfiguration verwenden, GuardDuty um eine SSM-Zuordnung für eine neue Instance zu erstellen, stellen Sie sicher, dass die neue Instance SSM-verwaltet wird und unter Fleet Manager in der https://console.aws.amazon.com/systems-manager/ -Konsole angezeigt wird.
- Wenn Sie Ausschlusstags mit automatisierter Agentenkonfiguration verwenden:
  - Fügen Sie das `false` `TagGuardDutyManaged`: hinzu, bevor Sie den GuardDuty automatisierten Agenten für Ihr Konto konfigurieren.

    Stellen Sie sicher, dass Sie Ihren Amazon EC2 EC2-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für Amazon EC2 aktiviert haben, wird jede EC2-Instance, die ohne Ausschluss-Tag gestartet wird, von der GuardDuty automatisierten Agentenkonfiguration abgedeckt.
  - Damit die Ausnahmetags funktionieren, aktualisieren Sie die Instance-Konfiguration, sodass das Instance-Identitätsdokument im Instance-Metadaten-Service (IMDS) verfügbar ist. Das Verfahren Laufzeitüberwachung aktivieren für diesen Schritt ist bereits Teil Ihres Kontos.

CPU- und Speicherlimit für den GuardDuty Agenten

CPU-Grenze

Das maximale CPU-Limit für den GuardDuty Security Agent, der Amazon EC2 EC2-Instances zugeordnet ist, beträgt 10 Prozent der gesamten vCPU-Kerne. Wenn Ihre EC2-Instance beispielsweise über 4 vCPU-Kerne verfügt, kann der Security Agent maximal 40 Prozent der insgesamt verfügbaren 400 Prozent verwenden.

Speicherlimit

Aus dem Speicher, der Ihrer Amazon EC2 EC2-Instance zugeordnet ist, steht ein begrenzter Speicher zur Verfügung, den der GuardDuty Security Agent verwenden kann.

Die folgende Tabelle zeigt das Speicherlimit.

Speicher der Amazon EC2 EC2-Instance	Maximaler Arbeitsspeicher für den Agenten GuardDuty
Weniger als 8 GB	128 MB
Weniger als 32 GB	256 MB

Speicher der Amazon EC2 EC2-Instance	Maximaler Arbeitsspeicher für den Agenten GuardDuty
Mehr als oder gleich 32 GB	1 GB

Nächster Schritt

Der nächste Schritt besteht darin, Runtime Monitoring zu konfigurieren und auch den Security Agent (automatisch oder manuell) zu verwalten.

Voraussetzungen für den Support AWS Fargate (nur Amazon ECS)

Validierung der architektonischen Anforderungen

Die von Ihnen verwendete Plattform kann sich darauf auswirken, wie der GuardDuty Security Agent GuardDuty den Empfang der Runtime-Ereignisse von Ihren Amazon ECS-Clustern unterstützt. Sie müssen bestätigen, dass Sie eine der verifizierten Plattformen verwenden.

Erste Überlegungen:

- Die AWS Fargate (Fargate) Plattform für Ihre Amazon ECS-Cluster muss Linux sein. Die entsprechende Plattformversion muss mindestens`1.4.0`, oder sein`LATEST`. Weitere Informationen zu den Plattformversionen finden Sie unter Linux-Plattformversionen im Amazon Elastic Container Service Developer Guide.
- Die Windows-Plattformversionen werden noch nicht unterstützt.

Verifizierte Plattformen

Die Betriebssystemverteilung und die CPU-Architektur wirken sich auf die Unterstützung durch den GuardDuty Security Agent aus. Die folgende Tabelle zeigt die verifizierte Konfiguration für die Installation des GuardDuty Security Agents und die Konfiguration von Runtime Monitoring.

Betriebssystem-Verteilung	Kernel-Unterstützung	CPU-Architektur	
		x64 (AMD64)	Graviton (ARM64)
Linux	eBPF, Tracepoints, Kprobe	Unterstützt	Unterstützt

Geben Sie ECR-Berechtigungen und Subnetzdetails an

Bevor Sie Runtime Monitoring aktivieren, müssen Sie die folgenden Details angeben:

Stellen Sie eine Rolle zur Aufgabenausführung mit Berechtigungen bereit

Für die Rolle zur Aufgabenausführung benötigen Sie bestimmte Amazon Elastic Container Registry (Amazon ECR) -Berechtigungen. Sie können entweder die von AmazonECS TaskExecutionRolePolicy verwaltete Richtlinie verwenden oder Ihrer `TaskExecutionRole` Richtlinie die folgenden Berechtigungen hinzufügen:

```
...
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability",
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
...
```

Um die Amazon ECR-Berechtigungen weiter einzuschränken, können Sie den Amazon ECR-Repository-URI hinzufügen, der den GuardDuty Security Agent für hostet AWS Fargate (nur Amazon ECS). Weitere Informationen finden Sie unter Repository für GuardDuty Agenten auf AWS Fargate (nur Amazon ECS).

Geben Sie die Subnetzdetails in der Aufgabendefinition an

Sie können entweder die öffentlichen Subnetze als Eingabe in Ihrer Aufgabendefinition angeben oder einen Amazon ECR VPC-Endpunkt erstellen.

- Option zur Aufgabendefinition verwenden — Für die Ausführung der UpdateServiceAPIs CreateServiceund in der Amazon Elastic Container Service API-Referenz müssen Sie die Subnetzinformationen übergeben. Weitere Informationen finden Sie unter Amazon ECS-Aufgabendefinitionen im Amazon Elastic Container Service Developer Guide.
- Verwenden der Amazon ECR VPC-Endpunktoption — Netzwerkpfad zu Amazon ECR angeben — Stellen Sie sicher, dass der Amazon ECR-Repository-URI, der den GuardDuty Security Agent hostet, über das Netzwerk zugänglich ist. Wenn Ihre Fargate-Aufgaben in einem privaten Subnetz ausgeführt werden, benötigt Fargate den Netzwerkpfad, um den Container herunterzuladen. GuardDuty

  Informationen darüber, wie Fargate den GuardDuty Container herunterladen kann, finden Sie unter Using Amazon ECR with Amazon ECS im Amazon Elastic Container Service Developer Guide.

Überprüfung der Service-Kontroll-Richtlinie Ihres Unternehmens

Wenn Sie eine Service Control Policy (SCP) zur Verwaltung von Berechtigungen in Ihrer Organisation eingerichtet haben, stellen Sie sicher, dass die Richtlinie die Erlaubnis nicht verweigert. `guardduty:SendSecurityTelemetry` Sie ist erforderlich GuardDuty , um Runtime Monitoring für verschiedene Ressourcentypen zu unterstützen.

Wenn Sie ein Mitgliedskonto sind, stellen Sie eine Verbindung mit dem zugehörigen delegierten Administrator her. Informationen zur Verwaltung von SCPs für Ihre Organisation finden Sie unter Service Control Policies (SCPs).

CPU- und Arbeitsspeicherlimits

In der Fargate-Aufgabendefinition müssen Sie den CPU- und Speicherwert auf Taskebene angeben. Die folgende Tabelle zeigt die gültigen Kombinationen von CPU- und Speicherwerten auf Taskebene sowie die entsprechende maximale Speicherbegrenzung des GuardDuty Security Agents für den Container. GuardDuty

CPU-Wert	Speicherwert	GuardDuty maximale Speicherbegrenzung des Agents
256 (0,25 vCPU)	512 MiB, 1 GB, 2 GB	128 MB
512 (0,5 vCPU)	1 GB, 2 GB, 3 GB, 4 GB	
1024 (1 vCPU)	2 GB, 3 GB, 4 GB	
	5 GB, 6 GB, 7 GB, 8 GB	
2048 (2 vCPU)	Zwischen 4 GB und 16 GB in 1-GB-Schritten	
4096 (4 vCPU)	Zwischen 8 GB und 20 GB in Schritten von 1 GB	
8 192 (8 vCPU)	Zwischen 16 GB und 28 GB in Schritten von 4 GB	256 MB

CPU-Wert	Speicherwert	GuardDuty maximale Speicherbegrenzung des Agents
	Zwischen 32 GB und 60 GB in Schritten von 4 GB	512 MB
16384 (16 vCPU)	Zwischen 32 GB und 120 GB in 8-GB-Schritten	1 GB

Nachdem Sie Runtime Monitoring aktiviert und festgestellt haben, dass der Abdeckungsstatus Ihres Clusters fehlerfrei ist, können Sie die Container Insight-Metriken einrichten und anzeigen. Weitere Informationen finden Sie unter Überwachung auf dem Amazon ECS-Cluster einrichten.

Der nächste Schritt besteht darin, Runtime Monitoring und auch den Security Agent zu konfigurieren.

Voraussetzungen für die Unterstützung von Amazon EKS-Clustern

Validierung der architektonischen Anforderungen

Die von Ihnen verwendete Plattform kann sich darauf auswirken, wie der GuardDuty Security Agent den Empfang von Runtime-Ereignissen von Ihren EKS-Clustern unterstützt GuardDuty . Sie müssen bestätigen, dass Sie eine der verifizierten Plattformen verwenden. Wenn Sie den GuardDuty Agenten manuell verwalten, stellen Sie sicher, dass die Kubernetes-Version die GuardDuty Agentenversion unterstützt, die derzeit verwendet wird.

Verifizierte Plattformen

Die Betriebssystemverteilung, die Kernel-Version und die CPU-Architektur wirken sich auf die vom GuardDuty Security Agent bereitgestellte Unterstützung aus. Die folgende Tabelle zeigt die verifizierte Konfiguration für die Installation des GuardDuty Security Agents und die Konfiguration von EKS Runtime Monitoring.

Betriebssystem-Verteilung	Kernel-Version	Kernel-Unterstützung	CPU-Architektur	Unterstützte Kubernetes-Version

			x64 (AMD64)	Graviton (ARM64) (Graviton2 und höher) [1]	
Ubuntu AL 2 AL 2023 [3]	5.4, 5.10, 5.15, 6.1 [2]	eBPF-Tracepoints, Kprobe	Unterstützt	Unterstützt	v1.21 - v1.29
Bottlerocket					v1.23 - v1.29

1. Runtime Monitoring für Amazon EKS-Cluster unterstützt Graviton-Instances der ersten Generation wie A1-Instance-Typen nicht.
2. Derzeit können mit der Kernel-Version keine `6.1` Generierungen GuardDuty vorgenommen werden, Runtime Monitoring: Typen finden die sich auf Folgendes beziehen. DNS-Ereignisse
3. Runtime Monitoring unterstützt AL2023 mit der Version des GuardDuty Security Agents v1.6.0 und höher. Weitere Informationen finden Sie unter GuardDuty Sicherheitsagent für Amazon EKS-Cluster.

Kubernetes-Versionen, die vom Security Agent unterstützt werden GuardDuty

Die folgende Tabelle zeigt die Kubernetes-Versionen für Ihre EKS-Cluster, die vom Security Agent unterstützt werden. GuardDuty

Kubernetes-Version	Version des Amazon GuardDuty EKS-Zusatz-Sicherheitsagenten									
	v1.6.1	v1.6.0	v1.5.0	v1.4.1	v1.4.0	v1.3.1	v1.3.0	v1.2.0	v1.1.0	v1.0.0
1,29	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

1,28	Unterstützt	Unterstützt
1,27		Unterstützt
1,26		Unterstützt
1,25		Unterstützt
1,24		
1,23		
1,22		
1,21		

Für einige Versionen des GuardDuty Security Agents wird der Standardsupport auslaufen. Informationen zu den Release-Versionen der Agenten finden Sie unterGuardDuty Sicherheitsagent für Amazon EKS-Cluster.

CPU- und Arbeitsspeicherlimits

Die folgende Tabelle zeigt die CPU- und Speicherlimits für das Amazon EKS-Add-on für GuardDuty (`aws-guardduty-agent`).

Parameter	Minimale Grenze	Maximale Grenze
CPU	200m	1000m
Arbeitsspeicher	256 Mi	1024Mi

Wenn Sie Amazon EKS Add-on Version 1.5.0 oder höher verwenden, GuardDuty bietet es die Möglichkeit, das Add-On-Schema für Ihre CPU- und Speicherwerte zu konfigurieren. Informationen zum konfigurierbaren Bereich finden Sie unterKonfigurierbare Parameter und Werte.

Nachdem Sie die EKS-Laufzeit-Überwachung aktiviert und den Abdeckungsstatus Ihrer EKS-Cluster bewertet haben, können Sie die Container-Erkenntnis-Metriken einrichten und anzeigen. Weitere Informationen finden Sie unter Einrichten der CPU- und Arbeitsspeicherüberwachung.

Nächster Schritt

Der nächste Schritt besteht darin, Runtime Monitoring zu konfigurieren und den Security Agent entweder manuell oder automatisch zu verwalten GuardDuty.

Runtime Monitoring für ein eigenständiges Konto aktivieren

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Wählen Sie auf der Registerkarte Konfiguration die Option Aktivieren aus, um Runtime Monitoring für Ihr Konto zu aktivieren.
4. GuardDuty Um Runtime-Ereignisse von einem oder mehreren Ressourcentypen — einer Amazon EC2 EC2-Instance, einem Amazon ECS-Cluster oder einem Amazon EKS-Cluster — zu empfangen, verwenden Sie die folgenden Optionen, um den Security Agent für diese Ressourcen zu verwalten:

   Um den GuardDuty Security Agent zu aktivieren

   - Verwaltung des automatisierten Sicherheitsagenten für Amazon EC2 EC2-Instance
   - Manuelles Verwalten des Security Agents für Amazon EC2 EC2-Instance
   - Verwaltung eines automatisierten Sicherheitsagenten für Fargate (nur Amazon ECS)
   - Automatisches Verwalten des Security Agents für Amazon EKS-Cluster
   - Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster

Runtime Monitoring für Umgebungen mit mehreren Konten aktivieren

In Umgebungen mit mehreren Konten kann nur das delegierte GuardDuty Administratorkonto die Laufzeitüberwachung für die Mitgliedskonten aktivieren oder deaktivieren und die automatische Agentenkonfiguration für die Ressourcentypen verwalten, die zu den Mitgliedskonten in ihrer Organisation gehören. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten.

Für ein delegiertes Administratorkonto GuardDuty

Um Runtime Monitoring für ein delegiertes GuardDuty Administratorkonto zu aktivieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Wählen Sie auf der Registerkarte Konfiguration im Abschnitt Runtime Monitoring-Konfiguration die Option Bearbeiten aus.
4. Verwendung von Für alle Konten aktivieren

   Wenn Sie Runtime Monitoring für alle Konten aktivieren möchten, die zur Organisation gehören, einschließlich des delegierten GuardDuty Administratorkontos, wählen Sie Für alle Konten aktivieren aus.
5. Verwendung von Konten manuell konfigurieren

   Wenn Sie Runtime Monitoring für jedes Mitgliedskonto einzeln aktivieren möchten, wählen Sie Konten manuell konfigurieren.

   - Wählen Sie im Abschnitt Delegierter Administrator (dieses Konto) die Option Aktivieren.
6. GuardDuty Um Runtime-Ereignisse von einem oder mehreren Ressourcentypen — einer Amazon EC2 EC2-Instance, einem Amazon ECS-Cluster oder einem Amazon EKS-Cluster — zu empfangen, verwenden Sie die folgenden Optionen, um den Security Agent für diese Ressourcen zu verwalten:

   Um den GuardDuty Security Agent zu aktivieren

   - Verwaltung des automatisierten Sicherheitsagenten für Amazon EC2 EC2-Instance
   - Manuelles Verwalten des Security Agents für Amazon EC2 EC2-Instance
   - Verwaltung eines automatisierten Sicherheitsagenten für Fargate (nur Amazon ECS)
   - Automatisches Verwalten des Security Agents für Amazon EKS-Cluster
   - Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster

Für alle Mitgliedskonten

Um Runtime Monitoring für alle Mitgliedskonten in der Organisation zu aktivieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit dem delegierten GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Wählen Sie auf der Seite Runtime Monitoring auf der Registerkarte Konfiguration im Abschnitt Runtime Monitoring-Konfiguration die Option Bearbeiten aus.
4. Wählen Sie Für alle Konten aktivieren.
5. GuardDuty Um Runtime-Ereignisse von einem oder mehreren Ressourcentypen — einer Amazon EC2 EC2-Instance, einem Amazon ECS-Cluster oder einem Amazon EKS-Cluster — zu empfangen, verwenden Sie die folgenden Optionen, um den Security Agent für diese Ressourcen zu verwalten:

   Um den GuardDuty Security Agent zu aktivieren

   - Verwaltung des automatisierten Sicherheitsagenten für Amazon EC2 EC2-Instance
   - Manuelles Verwalten des Security Agents für Amazon EC2 EC2-Instance
   - Verwaltung eines automatisierten Sicherheitsagenten für Fargate (nur Amazon ECS)
   - Automatisches Verwalten des Security Agents für Amazon EKS-Cluster
   - Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster

Für alle bestehenden aktiven Mitgliedskonten

Um Runtime Monitoring für bestehende Mitgliedskonten in der Organisation zu aktivieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit dem delegierten GuardDuty Administratorkonto für die Organisation an.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Auf der Runtime Monitoring-Seite können Sie auf der Registerkarte Konfiguration den aktuellen Status der Runtime Monitoring-Konfiguration einsehen.

4. Wählen Sie im Bereich Runtime Monitoring im Abschnitt Aktive Mitgliedskonten die Option Aktionen aus.
5. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
6. Wählen Sie Bestätigen aus.
7. GuardDuty Um Runtime-Ereignisse von einem oder mehreren Ressourcentypen — einer Amazon EC2 EC2-Instance, einem Amazon ECS-Cluster oder einem Amazon EKS-Cluster — zu empfangen, verwenden Sie die folgenden Optionen, um den Security Agent für diese Ressourcen zu verwalten:

   Um den GuardDuty Security Agent zu aktivieren

   - Verwaltung des automatisierten Sicherheitsagenten für Amazon EC2 EC2-Instance
   - Manuelles Verwalten des Security Agents für Amazon EC2 EC2-Instance
   - Verwaltung eines automatisierten Sicherheitsagenten für Fargate (nur Amazon ECS)
   - Automatisches Verwalten des Security Agents für Amazon EKS-Cluster
   - Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Automatische Aktivierung der Laufzeitüberwachung nur für neue Mitgliedskonten

Um Runtime Monitoring für neue Mitgliedskonten in Ihrer Organisation zu aktivieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit dem designierten delegierten GuardDuty Administratorkonto der Organisation an.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus
3. Wählen Sie auf der Registerkarte Konfiguration im Abschnitt Runtime Monitoring-Konfiguration die Option Bearbeiten aus.
4. Wählen Sie Konten manuell konfigurieren.

5. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren.
6. GuardDuty Um Runtime-Ereignisse von einem oder mehreren Ressourcentypen — einer Amazon EC2 EC2-Instance, einem Amazon ECS-Cluster oder einem Amazon EKS-Cluster — zu empfangen, verwenden Sie die folgenden Optionen, um den Security Agent für diese Ressourcen zu verwalten:

   Um den GuardDuty Security Agent zu aktivieren

   - Verwaltung des automatisierten Sicherheitsagenten für Amazon EC2 EC2-Instance
   - Manuelles Verwalten des Security Agents für Amazon EC2 EC2-Instance
   - Verwaltung eines automatisierten Sicherheitsagenten für Fargate (nur Amazon ECS)
   - Automatisches Verwalten des Security Agents für Amazon EKS-Cluster
   - Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster

Nur für ausgewählte aktive Mitgliedskonten

Um die Laufzeitüberwachung für einzelne aktive Mitgliedskonten zu aktivieren

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldeinformationen für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Überprüfen Sie auf der Seite Konten die Werte in den Spalten Runtime Monitoring und Agent automatisch verwalten. Diese Werte geben an, ob Runtime Monitoring und GuardDuty Agentenverwaltung für das entsprechende Konto aktiviert oder nicht aktiviert sind.
4. Wählen Sie in der Tabelle Konten das Konto aus, für das Sie Runtime Monitoring aktivieren möchten. Sie können mehrere Konten gleichzeitig auswählen.
5. Wählen Sie Bestätigen aus.
6. Wählen Sie Schutzpläne bearbeiten aus. Wählen Sie die geeignete Aktion aus.
7. Wählen Sie Bestätigen aus.
8. GuardDuty Um Runtime-Ereignisse von einem oder mehreren Ressourcentypen — einer Amazon EC2 EC2-Instance, einem Amazon ECS-Cluster oder einem Amazon EKS-Cluster — zu empfangen, verwenden Sie die folgenden Optionen, um den Security Agent für diese Ressourcen zu verwalten:

Um den GuardDuty Security Agent zu aktivieren

- Verwaltung des automatisierten Sicherheitsagenten für Amazon EC2 EC2-Instance
- Manuelles Verwalten des Security Agents für Amazon EC2 EC2-Instance
- Verwaltung eines automatisierten Sicherheitsagenten für Fargate (nur Amazon ECS)
- Automatisches Verwalten des Security Agents für Amazon EKS-Cluster
- Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster

Verwaltung von GuardDuty Security Agents

Sie können den GuardDuty Security Agent für die Ressource verwalten, die Sie überwachen möchten. Wenn Sie mehr als einen Ressourcentyp überwachen möchten, stellen Sie sicher, dass Sie den GuardDuty Agenten für diese Ressource verwalten.

> **Important**
>
> Wenn Sie mit einem GuardDuty Security Agent für eine Amazon EC2 EC2-Instance arbeiten, können Sie den Agenten auf dem zugrunde liegenden Host innerhalb eines Amazon EKS-Clusters installieren und verwenden. Wenn Sie bereits einen Security Agent auf diesem EKS-Cluster installiert haben, könnten auf demselben Host zwei Security Agents gleichzeitig ausgeführt werden. Informationen zur GuardDuty Funktionsweise in diesem Szenario finden Sie unterUmgang mit dualen Sicherheitsagenten.

Die folgenden Themen helfen Ihnen bei den nächsten Schritten zur Verwaltung des Security Agents.

Inhalt

- Verwenden einer gemeinsam genutzten VPC mit automatisierten Sicherheitsagenten
- Umgang mit auf einem Host installierten Dual-Security-Agents
- Verwaltung des automatisierten Sicherheitsagenten für Amazon EC2 EC2-Instance
- Manuelles Verwalten des Security Agents für Amazon EC2 EC2-Instance
- Verwaltung eines automatisierten Sicherheitsagenten für Fargate (nur Amazon ECS)
- Automatisches Verwalten des Security Agents für Amazon EKS-Cluster
- Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster

Verwenden einer gemeinsam genutzten VPC mit automatisierten Sicherheitsagenten

Wenn Sie den Security Agent automatisch verwalten GuardDuty möchten, unterstützt Runtime Monitoring die Verwendung einer gemeinsam genutzten VPC für AWS-Konten diejenigen, die derselben Organisation angehören. AWS Organizations GuardDuty Kann in Ihrem Namen die Amazon VPC-Endpunktrichtlinie auf der Grundlage der Details festlegen, die mit der gemeinsam genutzten VPC für Ihre Organisation verknüpft sind.

Vor dieser Version wurde die Verwendung gemeinsam genutzter VPCs nur GuardDuty unterstützt, wenn Sie den GuardDuty Security Agent manuell verwalten wollten.

Inhalt

Funktionsweise

Wenn das Besitzerkonto der gemeinsam genutzten VPC Runtime Monitoring und automatische Agentenkonfiguration für eine der Ressourcen (Amazon EKS oder AWS Fargate (nur Amazon ECS)) aktiviert, kommen alle gemeinsam genutzten VPCs für die automatische Installation des gemeinsamen Amazon VPC-Endpunkts und der zugehörigen Sicherheitsgruppe im gemeinsamen VPC-Eigentümerkonto in Frage. GuardDuty ruft die Organisations-ID ab, die mit der gemeinsam genutzten Amazon VPC verknüpft ist.

Jetzt können diejenigen, AWS-Konten die derselben Organisation angehören wie das gemeinsame Amazon VPC-Besitzerkonto, auch denselben Amazon VPC-Endpunkt nutzen. GuardDuty erstellt die gemeinsame VPC, wenn entweder das gemeinsame VPC-Eigentümerkonto oder das teilnehmende Konto einen Amazon VPC-Endpunkt benötigt. Beispiele für die Notwendigkeit eines Amazon VPC-Endpunkts sind die Aktivierung GuardDuty, Runtime Monitoring, EKS Runtime Monitoring oder das Starten einer neuen Amazon ECS-Fargate-Aufgabe. Wenn diese Konten Runtime Monitoring und automatische Agentenkonfiguration für einen beliebigen Ressourcentyp aktivieren, GuardDuty wird ein Amazon VPC-Endpunkt erstellt und die Endpunktrichtlinie mit derselben Organisations-ID wie die des gemeinsamen VPC-Besitzerkontos festgelegt. GuardDuty fügt ein `GuardDutyManaged` Tag hinzu und setzt es `true` für den Amazon VPC-Endpunkt, der GuardDuty erstellt, auf. Wenn das gemeinsame Amazon VPC-Besitzerkonto weder Runtime Monitoring noch automatische Agentenkonfiguration für eine der Ressourcen aktiviert hat, GuardDuty wird die Amazon VPC-Endpunktrichtlinie nicht festgelegt. Informationen zur Konfiguration von Runtime Monitoring und zur

automatischen Verwaltung des Security Agents im gemeinsamen VPC-Besitzerkonto finden Sie unter GuardDuty Runtime Monitoring aktivieren.

Jedes Konto, das dieselbe Amazon VPC-Endpunktrichtlinie verwendet, wird als AWS Teilnehmerkonto der zugehörigen gemeinsamen Amazon VPC bezeichnet.

Das folgende Beispiel zeigt die Standard-VPC-Endpunktrichtlinie des gemeinsamen VPC-Besitzerkontos und des Teilnehmerkontos. Das `aws:PrincipalOrgID` zeigt die Organisations-ID an, die der gemeinsam genutzten VPC-Ressource zugeordnet ist. Die Verwendung dieser Richtlinie ist auf die Teilnehmerkonten beschränkt, die in der Organisation des Eigentümerkontos vorhanden sind.

Example

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "*",
            "Resource": "*",
            "Effect": "Allow",
            "Principal": "*"
        },
        {
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalOrgID": "o-abcdef0123"
                }
            },
            "Action": "*",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "*"
        }
    ]
}
```

Voraussetzungen für die Verwendung von Shared VPC

Voraussetzungen für die Ersteinrichtung

Führen Sie die folgenden Schritte in dem aus AWS-Konto , in dem Sie Eigentümer der gemeinsam genutzten VPC sein möchten:

1. Organisation erstellen — Erstellen Sie eine Organisation, indem Sie die Schritte unter Organisation erstellen und verwalten im AWS Organizations Benutzerhandbuch befolgen.

   Informationen zum Hinzufügen oder Entfernen von Mitgliedskonten finden Sie unter Verwaltung AWS-Konten in Ihrer Organisation.

2. Eine gemeinsam genutzte VPC-Ressource erstellen — Sie können eine gemeinsam genutzte VPC-Ressource über das Besitzerkonto erstellen. Weitere Informationen finden Sie unter Freigeben Ihrer VPC für andere Konten im Amazon-VPC-Benutzerhandbuch.

Spezifische Voraussetzungen für Runtime Monitoring GuardDuty

Die folgende Liste enthält die spezifischen Voraussetzungen für GuardDuty:

- Das Besitzerkonto der gemeinsam genutzten VPC und das teilnehmende Konto können von verschiedenen Organisationen in GuardDuty stammen. Sie müssen jedoch derselben Organisation in AWS Organizations angehören. Dies ist erforderlich GuardDuty , um einen Amazon VPC-Endpunkt und eine Sicherheitsgruppe für die gemeinsam genutzte VPC zu erstellen. Informationen zur Funktionsweise gemeinsam genutzter VPCs finden Sie unter Teilen Sie Ihre VPC mit anderen Konten im Amazon VPC-Benutzerhandbuch.
- Aktivieren Sie Runtime Monitoring oder EKS Runtime Monitoring und die GuardDuty automatische Agentenkonfiguration für jede Ressource im gemeinsamen VPC-Besitzerkonto und im Teilnehmerkonto. Weitere Informationen finden Sie unter Laufzeitüberwachung aktivieren.

  Wenn Sie diese Konfigurationen bereits abgeschlossen haben, fahren Sie mit dem nächsten Schritt fort.
- Wenn Sie entweder mit einer Amazon EKS- oder einer Amazon ECS-Aufgabe (AWS Fargate nur) arbeiten, stellen Sie sicher, dass Sie die gemeinsam genutzte VPC-Ressource auswählen, die dem Besitzerkonto zugeordnet ist, und wählen Sie deren Subnetze aus.

Häufig gestellte Fragen (FAQ)

Die folgende Liste enthält die Schritte zur Fehlerbehebung bei häufig gestellten Fragen bei der Verwendung einer gemeinsam genutzten VPC-Ressource mit aktivierter GuardDuty automatisierter Agentenkonfiguration in Runtime Monitoring:

Ich verwende bereits Runtime Monitoring (oder EKS Runtime Monitoring). Wie aktiviere ich Shared VPC?

Informationen zu den Voraussetzungen für die Erstellung einer gemeinsam genutzten VPC finden Sie unterVoraussetzungen.

Wenn sowohl das gemeinsame VPC-Besitzerkonto als auch das Teilnehmerkonto die Voraussetzungen erfüllen, GuardDuty wird versucht, die Amazon VPC-Endpunktrichtlinie automatisch festzulegen.

Wenn Sie vor dieser Version ein Problem mit der Abdeckung AWS-Konto hatten, weil die gemeinsam genutzte VPC nicht unterstützt wurde, befolgen Sie die Voraussetzungen. Wenn Ihr Ressourcentyp (Amazon EKS oder Amazon ECS-Aufgabe (AWS Fargate nur)) die Anforderung eines gemeinsamen VPC-Endpunkts aufruft, GuardDuty wird versucht, die neue VPC-Endpunktrichtlinie festzulegen.

Als gemeinsam genutztes VPC-Besitzerkonto möchte ich, dass die gemeinsame VPC-Endpunktrichtlinie auf eine Teilmenge von Teilnehmerkonten in meiner Organisation beschränkt wird. Wie kann ich das tun?

Wenn dem Endpunkt ein`GuardDutyManaged`: `true` -Tag zugeordnet ist, entfernen Sie es. Dadurch wird verhindert GuardDuty , dass versucht wird, die VPC-Endpunktrichtlinie der gemeinsam genutzten VPC zu ändern oder zu überschreiben.

Weitere Informationen finden Sie unter Steuern des Zugriffs auf VPC-Endpoints mithilfe von Endpunktrichtlinien.

Warum ändert sich der gemeinsam genutzte VPC-Endpunkt von **`aws:PrincipalAccount`** zu**`aws:PrincipalOrgId`**? Wie kann ich das verhindern?

Wenn GuardDuty erkannt wird, dass die VPC von mehreren Konten derselben Organisation gemeinsam genutzt wird AWS Organizations, GuardDuty versucht, die Richtlinie so zu ändern, dass die Organisations-ID angegeben wird.

Um dies zu verhindern, entfernen Sie das `true` Tag`GuardDutyManaged`: vom gemeinsam genutzten VPC-Endpunkt. Dadurch wird verhindert GuardDuty , dass versucht wird, die VPC-Endpunktrichtlinie der gemeinsam genutzten VPC zu ändern oder zu überschreiben.

Was passiert, wenn das gemeinsame VPC-Besitzerkonto oder eines der Teilnehmerkonten Runtime Monitoring (GuardDuty oder EKS Runtime Monitoring) deaktiviert?

Wenn das gemeinsame VPC-Besitzerkonto GuardDuty oder Runtime Monitoring (oder EKS Runtime Monitoring) deaktiviert, wird GuardDuty geprüft, ob ein Ressourcentyp, der zum Teilnehmerkonto

gehört, den gemeinsamen VPC-Endpunkt verwendet hat oder ob ein Teilnehmerkonto jemals die GuardDuty Agentenverwaltung für einen beliebigen Ressourcentyp aktiviert hat. Falls ja, GuardDuty werden der VPC-Endpunkt und die Sicherheitsgruppe nicht gelöscht.

Wenn das gemeinsame VPC-Teilnehmerkonto GuardDuty oder Runtime Monitoring (oder EKS Runtime Monitoring) deaktiviert, hat dies keine Auswirkungen auf das gemeinsame VPC-Besitzerkonto und das Besitzerkonto löscht weder die gemeinsam genutzte VPC-Ressource noch die Sicherheitsgruppe.

Wie kann ich die gemeinsam genutzte VPC-Ressource löschen? Welche Auswirkungen wird es haben?

Als gemeinsam genutztes VPC-Besitzerkonto können Sie die gemeinsam genutzte VPC-Ressource löschen, auch wenn sie von Ihrem Konto oder einem der teilnehmenden Konten in Runtime Monitoring verwendet wird. Informationen zum Löschen der gemeinsam genutzten VPC und zu ihren Auswirkungen finden Sie unterTo delete a VPC endpoint.

Umgang mit auf einem Host installierten Dual-Security-Agents

Amazon EC2 EC2-Instances können mehrere Arten von Workloads unterstützen. Wenn Sie einen automatisierten Security Agent auf einer Amazon EC2 EC2-Instance konfigurieren, verfügt dieselbe EC2-Instance möglicherweise über EKS über einen anderen Security Agent.

Übersicht

Stellen Sie sich ein Szenario vor, in dem Sie Runtime Monitoring aktiviert haben. Jetzt aktivieren Sie den automatisierten Agenten für Amazon EKS über GuardDuty. Sie haben auch den automatisierten Agenten für Amazon EC2 aktiviert. Es kann vorkommen, dass derselbe zugrunde liegende Host mit zwei Security Agents installiert wird — einer für Amazon EKS und der andere für Amazon EC2. Dies kann dazu führen, dass zwei Security Agents auf demselben Host laufen, Laufzeitereignisse sammeln und an GuardDuty diese senden und möglicherweise doppelte Ergebnisse generieren.

Auswirkung

- Wenn mehr als ein Security Agent auf demselben Host ausgeführt wird, kann es sein, dass Ihr Konto doppelt so viel CPU- und Speicherverarbeitung benötigt. Informationen zu den CPU- und Speicherlimits für jeden Ressourcentyp finden Sie unter Voraussetzungen für diese Ressource.
- GuardDuty hat die Runtime Monitoring-Funktion so konzipiert, dass Ihr Konto nur für einen Stream von Runtime-Ereignissen belastet wird, selbst wenn sich zwei Security Agents überschneiden, die Runtime-Ereignisse von demselben zugrundeliegenden Host sammeln.

Wie GuardDuty geht man mit mehreren Agenten um

GuardDuty erkennt, wenn zwei Security Agents auf demselben Host laufen, und bestimmt nur einen davon als Security Agent, der aktiv Runtime-Ereignisse sammelt. Der zweite Agent verbraucht nur minimale Systemressourcen, um jegliche Beeinträchtigung der Leistung Ihrer Anwendungen zu verhindern.

GuardDuty berücksichtigt die folgenden Szenarien:

- Wenn eine EC2-Instance sowohl in den Geltungsbereich von Amazon EKS als auch von Amazon EC2-Sicherheitsagenten fällt, hat der EKS-Sicherheitsagent Vorrang. Dies gilt nur, wenn Sie den Security Agent v1.1.0 oder höher für Amazon EC2 verwenden. Ältere Agentenversionen werden weiterhin ausgeführt und sammeln Runtime-Ereignisse, da ältere Agentenversionen von der Priorisierung nicht betroffen sind.
- Wenn sowohl Amazon EKS als auch Amazon EC2 Security Agents GuardDuty verwaltet haben und Ihre Amazon EC2 EC2-Instance ebenfalls SSM-verwaltet wird, werden beide Security Agents auf Host-Ebene installiert. Sobald die Agenten installiert sind, wird GuardDuty entschieden, welcher Security Agent weiter ausgeführt wird. Wenn beide Security Agents ausgeführt werden, sammelt letztendlich nur einer von ihnen Runtime-Ereignisse.
- Wenn die Security Agents, die sowohl EC2 als auch EKS zugeordnet sind, gleichzeitig ausgeführt werden, GuardDuty kann es nur während der Überschneidungszeit zu doppelten Ergebnissen kommen.

  Dies kann passieren, wenn:

  - Security Agents für EC2 und EKS werden GuardDuty (automatisch) konfiguriert, oder
  - Ihre Amazon EKS-Ressource verfügt über einen automatisierten Sicherheitsagenten.
- Wenn der EKS Security Agent bereits läuft und Sie den EC2 Security Agent manuell auf demselben zugrunde liegenden Host bereitstellen und alle Voraussetzungen erfüllen, wird GuardDuty möglicherweise kein zweiter Security Agent installiert.

Verwaltung des automatisierten Sicherheitsagenten für Amazon EC2 EC2-Instance

> **Note**
>
> Bevor Sie fortfahren, stellen Sie sicher, dass Sie alle Anweisungen befolgen. Voraussetzungen für die Unterstützung von Amazon EC2 EC2-Instances

Migration vom manuellen Amazon EC2 EC2-Agenten zum automatisierten Agenten

Dieser Abschnitt gilt für den AWS-Konto Fall, dass Sie den Security Agent zuvor manuell verwaltet haben und jetzt die GuardDuty automatische Agentenkonfiguration verwenden möchten. Falls dies nicht auf Sie zutrifft, fahren Sie mit der Konfiguration des Security Agents für Ihr Konto fort.

Wenn Sie den GuardDuty Automated Agent aktivieren, GuardDuty verwaltet er den Security Agent in Ihrem Namen. Informationen darüber, welche GuardDuty Schritte erforderlich sind, finden Sie unterVerwenden Sie die automatische Agentenkonfiguration (empfohlen).

Bereinigen von -Ressourcen

SSM-Zuordnung löschen

- Löschen Sie alle SSM-Verknüpfungen, die Sie möglicherweise erstellt haben, als Sie den Security Agent für Amazon EC2 manuell verwaltet haben. Weitere Informationen finden Sie unter Verknüpfungen löschen.
- Dies geschieht, damit Sie die Verwaltung von SSM-Aktionen übernehmen GuardDuty können, unabhängig davon, ob Sie automatisierte Agenten auf Konto- oder Instanzebene verwenden (mithilfe von Inklusions- oder Ausschlusstags). Weitere Informationen darüber, welche SSM-Aktionen ausführen können, GuardDuty finden Sie unter. Mit dem Dienst verknüpfte Rollenberechtigungen für GuardDuty
- Wenn Sie eine SSM-Verknüpfung löschen, die zuvor für die manuelle Verwaltung des Security Agents erstellt wurde, kann es bei GuardDuty der Erstellung einer SSM-Verknüpfung zur automatischen Verwaltung des Security Agents zu einer kurzen Überschneidung kommen. Während dieses Zeitraums kann es aufgrund der SSM-Planung zu Konflikten kommen. Weitere Informationen finden Sie unter Amazon EC2 SSM-Planung.

Einschluss- und Ausschluss-Tags für Ihre Amazon EC2 EC2-Instances verwalten

- Inclusion-Tags — Wenn Sie die GuardDuty automatische Agentenkonfiguration nicht aktivieren, sondern eine Ihrer Amazon EC2 EC2-Instances mit einem Inclusion-Tag (`GuardDutyManaged:true`) kennzeichnen, wird eine SSM-Zuordnung GuardDuty erstellt, die den Security Agent auf den ausgewählten EC2-Instances installiert und verwaltet. Dies ist ein erwartetes Verhalten, das Ihnen hilft, den Security Agent nur auf ausgewählten EC2-Instances zu verwalten. Weitere Informationen finden Sie unter So funktioniert Runtime Monitoring mit Amazon EC2 EC2-Instances.

  Um die Installation und Verwaltung des Security Agents zu GuardDuty verhindern, entfernen Sie das Inclusion-Tag von diesen EC2-Instances. Weitere Informationen finden Sie unter

Hinzufügen und Löschen von Tags im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

- Ausschluss-Tags — Wenn Sie die GuardDuty automatische Agentenkonfiguration für alle EC2-Instances in Ihrem Konto aktivieren möchten, stellen Sie sicher, dass keine EC2-Instance mit einem Ausschluss-Tag (:) `GuardDutyManaged` gekennzeichnet ist. `false`

Den GuardDuty Agenten für ein eigenständiges Konto konfigurieren

Configure for all instances

Um Runtime Monitoring für alle Instanzen in Ihrem eigenständigen Konto zu konfigurieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Wählen Sie auf der Registerkarte Konfiguration die Option Bearbeiten aus.
4. Wählen Sie im Abschnitt EC2 die Option Aktivieren aus.
5. Wählen Sie Speichern.
6. Sie können überprüfen, ob die SSM-Verknüpfung, die GuardDuty erstellt wird, den Security Agent auf allen EC2-Ressourcen installiert und verwaltet, die zu Ihrem Konto gehören.

   a. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.

   b. Öffnen Sie die Registerkarte Ziele für die SSM-Zuordnung (`GuardDutyRuntimeMonitoring-do-not-delete`). Beachten Sie, dass der Tag-Schlüssel als InstanceIdsangezeigt wird.

Using inclusion tag in selected instances

So konfigurieren Sie den GuardDuty Security Agent für ausgewählte Amazon EC2 EC2-Instances

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `true` Tag`GuardDutyManaged`: hinzu. Informationen zum

Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.

3. Sie können überprüfen, ob die SSM-Zuordnung, die GuardDuty erstellt wird, den Security Agent nur auf den EC2-Ressourcen installiert und verwaltet, die mit den Inklusion-Tags gekennzeichnet sind.

   Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.

   - Öffnen Sie die Registerkarte Ziele für die SSM-Assoziation, die erstellt wird (`GuardDutyRuntimeMonitoring-do-not-delete`). Der Tag-Schlüssel wird als Tag: GuardDutyManaged angezeigt.

Using exclusion tag in selected instances

> **Note**
>
> Stellen Sie sicher, dass Sie Ihren Amazon EC2 EC2-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für Amazon EC2 aktiviert haben, wird jede EC2-Instance, die ohne Ausschluss-Tag gestartet wird, von der GuardDuty automatisierten Agentenkonfiguration abgedeckt.

So konfigurieren Sie den GuardDuty Security Agent für ausgewählte Amazon EC2 EC2-Instances

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie nicht überwachen und potenzielle Bedrohungen nicht erkennen GuardDuty möchten, das `false` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.
3. Gehen Sie wie folgt vor, damit die Ausschluss-Tags in den Instanz-Metadaten verfügbar sind:

   a. Sehen Sie sich auf dem Tab Details Ihrer Instance den Status für Tags zulassen in den Instanz-Metadaten an.

      Wenn es derzeit Deaktiviert ist, gehen Sie wie folgt vor, um den Status auf Aktiviert zu ändern. Andernfalls überspringen Sie diesen Schritt.

b. Wählen Sie die Instanz aus, für die Sie Tags zulassen möchten.
c. Wählen Sie im Menü Aktionen die Option Instanzeinstellungen aus.
d. Wähle „Tags in Instanz-Metadaten zulassen“.
e. Wählen Sie unter Zugriff auf Tags in Instanzmetadaten die Option Zulassen aus.
f. Wählen Sie Speichern.

4. Nachdem Sie das Ausschluss-Tag hinzugefügt haben, führen Sie dieselben Schritte aus, wie auf der Registerkarte Für alle Instanzen konfigurieren angegeben.

Sie können jetzt die Laufzeit beurteilen. Deckung für Amazon EC2 EC2-Instance

Konfiguration des GuardDuty Agenten in einer Umgebung mit mehreren Konten

Für ein delegiertes Administratorkonto GuardDuty

Configure for all instances

Wenn Sie für Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben, wählen Sie eine der folgenden Optionen für das delegierte GuardDuty Administratorkonto:

- Option 1

  Wählen Sie unter Automatisierte Agentenkonfiguration im Abschnitt EC2 die Option Für alle Konten aktivieren aus.
- Option 2
  - Wählen Sie unter Automatisierte Agentenkonfiguration im Abschnitt EC2 die Option Konten manuell konfigurieren aus.
  - Wählen Sie unter Delegierter Administrator (dieses Konto) die Option Aktivieren aus.
- Wählen Sie Speichern.

Wenn Sie Konten manuell für Runtime Monitoring konfigurieren ausgewählt haben, führen Sie die folgenden Schritte aus:

- Wählen Sie unter Automatisierte Agentenkonfiguration im Abschnitt EC2 die Option Konten manuell konfigurieren aus.
- Wählen Sie unter Delegierter Administrator (dieses Konto) die Option Aktivieren aus.
- Wählen Sie Speichern.

Unabhängig davon, welche Option Sie wählen, um die automatische Agentenkonfiguration für das delegierte GuardDuty Administratorkonto zu aktivieren, können Sie sicherstellen, dass die SSM-Zuordnung, die GuardDuty erstellt wird, den Security Agent auf allen EC2-Ressourcen installiert und verwaltet, die zu diesem Konto gehören.

1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Öffnen Sie die Registerkarte Ziele für die SSM-Zuordnung (`GuardDutyRuntimeMonitoring-do-not-delete`). Beachten Sie, dass der Tag-Schlüssel als InstanceIdsangezeigt wird.

Using inclusion tag in selected instances

So konfigurieren Sie den GuardDuty Agenten für ausgewählte Amazon EC2 EC2-Instances

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `true` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.

   Durch Hinzufügen dieses Tags GuardDuty kann der Security Agent für diese ausgewählten EC2-Instances installiert und verwaltet werden. Sie müssen die automatische Agentenkonfiguration nicht explizit aktivieren.
3. Sie können überprüfen, ob die SSM-Verknüpfung, die GuardDuty erstellt wird, den Security Agent nur auf den EC2-Ressourcen installiert und verwaltet, die mit den Inclusion-Tags gekennzeichnet sind.

   Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.

   - Öffnen Sie die Registerkarte Ziele für die SSM-Assoziation, die erstellt wird (`GuardDutyRuntimeMonitoring-do-not-delete`). Der Tag-Schlüssel wird als Tag: GuardDutyManaged angezeigt.

Using exclusion tag in selected instances

> **Note**
>
> Stellen Sie sicher, dass Sie Ihren Amazon EC2 EC2-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für Amazon EC2 aktiviert haben, wird jede EC2-Instance, die ohne Ausschluss-Tag gestartet wird, von der GuardDuty automatisierten Agentenkonfiguration abgedeckt.

So konfigurieren Sie den GuardDuty Agenten für ausgewählte Amazon EC2 EC2-Instances

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie nicht überwachen und potenzielle Bedrohungen nicht erkennen GuardDuty möchten, das `false` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.
3. Gehen Sie wie folgt vor, damit die Ausschluss-Tags in den Instanz-Metadaten verfügbar sind:

   a. Sehen Sie sich auf dem Tab Details Ihrer Instance den Status für Tags zulassen in den Instanz-Metadaten an.

      Wenn es derzeit Deaktiviert ist, gehen Sie wie folgt vor, um den Status auf Aktiviert zu ändern. Andernfalls überspringen Sie diesen Schritt.

   b. Wählen Sie im Menü Aktionen die Option Instanzeinstellungen aus.

   c. Wähle „Tags in Instanz-Metadaten zulassen“.
4. Nachdem Sie das Ausschluss-Tag hinzugefügt haben, führen Sie dieselben Schritte aus, wie auf der Registerkarte Für alle Instanzen konfigurieren angegeben.

Sie können jetzt die Laufzeit beurteilenDeckung für Amazon EC2 EC2-Instance.

Automatische Aktivierung für alle Mitgliedskonten

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Configure for all instances

Bei den folgenden Schritten wird davon ausgegangen, dass Sie im Abschnitt Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben:

1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration für Amazon EC2 die Option Für alle Konten aktivieren aus.
2. Sie können überprüfen, ob die SSM-Verknüpfung, die (`GuardDutyRuntimeMonitoring-do-not-delete`) GuardDuty erstellt, den Security Agent auf allen EC2-Ressourcen installiert und verwaltet, die zu diesem Konto gehören.

   a. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
   b. Öffnen Sie die Registerkarte Ziele für die SSM-Verknüpfung. Beachten Sie, dass der Tag-Schlüssel als InstanceIdsangezeigt wird.

Using inclusion tag in selected instances

So konfigurieren Sie den GuardDuty Agenten für ausgewählte Amazon EC2 EC2-Instances

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den EC2-Instances, die Sie überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `true` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.

   Durch Hinzufügen dieses Tags GuardDuty kann der Security Agent für diese ausgewählten EC2-Instances installiert und verwaltet werden. Sie müssen die automatische Agentenkonfiguration nicht explizit aktivieren.
3. Sie können überprüfen, ob die SSM-Verknüpfung, die GuardDuty erstellt wird, den Security Agent auf allen EC2-Ressourcen installiert und verwaltet, die zu Ihrem Konto gehören.

   a. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
   b. Öffnen Sie die Registerkarte Ziele für die SSM-Zuordnung (`GuardDutyRuntimeMonitoring-do-not-delete`). Beachten Sie, dass der Tag-Schlüssel als InstanceIdsangezeigt wird.

Using exclusion tag in selected instances

> **Note**
>
> Stellen Sie sicher, dass Sie Ihren Amazon EC2 EC2-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für Amazon EC2 aktiviert haben, wird jede EC2-Instance, die ohne Ausschluss-Tag gestartet wird, von der GuardDuty automatisierten Agentenkonfiguration abgedeckt.

So konfigurieren Sie den GuardDuty Security Agent für ausgewählte Amazon EC2 EC2-Instances

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie nicht überwachen und potenzielle Bedrohungen nicht erkennen GuardDuty möchten, das `false` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.
3. Gehen Sie wie folgt vor, damit die Ausschluss-Tags in den Instanz-Metadaten verfügbar sind:
   a. Sehen Sie sich auf dem Tab Details Ihrer Instance den Status für Tags zulassen in den Instanz-Metadaten an.

      Wenn es derzeit Deaktiviert ist, gehen Sie wie folgt vor, um den Status auf Aktiviert zu ändern. Andernfalls überspringen Sie diesen Schritt.
   b. Wählen Sie im Menü Aktionen die Option Instanzeinstellungen aus.
   c. Wähle „Tags in Instanz-Metadaten zulassen“.
4. Nachdem Sie das Ausschluss-Tag hinzugefügt haben, führen Sie dieselben Schritte aus, wie auf der Registerkarte Für alle Instanzen konfigurieren angegeben.

Sie können jetzt die Laufzeit beurteilenDeckung für Amazon EC2 EC2-Instance.

Automatische Aktivierung nur für neue Mitgliedskonten

Das delegierte GuardDuty Administratorkonto kann die automatische Agentenkonfiguration für die Amazon EC2 EC2-Ressource so einrichten, dass sie automatisch für die neuen Mitgliedskonten aktiviert wird, wenn sie der Organisation beitreten.

Configure for all instances

Bei den folgenden Schritten wird davon ausgegangen, dass Sie im Abschnitt Runtime Monitoring die Option Automatisch für neue Mitgliedskonten aktivieren ausgewählt haben:

1. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
2. Wählen Sie auf der Seite Runtime Monitoring die Option Bearbeiten aus.
3. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Dieser Schritt stellt sicher, dass jedes Mal, wenn ein neues Konto Ihrer Organisation beitritt, die automatische Agentenkonfiguration für Amazon EC2 automatisch für das Konto aktiviert wird. Nur das delegierte GuardDuty Administratorkonto der Organisation kann diese Auswahl ändern.
4. Wählen Sie Speichern.

Wenn der Organisation ein neues Mitgliedskonto beitritt, wird diese Konfiguration automatisch für dieses Mitglied aktiviert. GuardDuty Um den Sicherheitsagenten für die Amazon EC2 EC2-Instances zu verwalten, die zu diesem neuen Mitgliedskonto gehören, müssen Sie sicherstellen, dass alle Voraussetzungen erfüllt Für eine EC2-Instance sind.

Wenn eine SSM-Zuordnung erstellt wird (`GuardDutyRuntimeMonitoring-do-not-delete`), können Sie überprüfen, ob die SSM-Zuordnung den Security Agent auf allen EC2-Instances installiert und verwaltet, die zu dem neuen Mitgliedskonto gehören.

- Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
- Öffnen Sie die Registerkarte Ziele für die SSM-Verknüpfung. Beachten Sie, dass der Tag-Schlüssel als InstanceIdsangezeigt wird.

Using inclusion tag in selected instances

Um den GuardDuty Security Agent für ausgewählte Instanzen in Ihrem Konto zu konfigurieren

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `true` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.

Wenn Sie dieses Tag hinzufügen GuardDuty , können Sie den Security Agent für diese ausgewählten Instanzen installieren und verwalten. Sie müssen die automatische Agentenkonfiguration nicht explizit aktivieren.

3. Sie können überprüfen, ob die SSM-Verknüpfung, die GuardDuty erstellt wird, den Security Agent nur auf den EC2-Ressourcen installiert und verwaltet, die mit den Inclusion-Tags gekennzeichnet sind.

   a. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.

   b. Öffnen Sie die Registerkarte Ziele für die SSM-Verknüpfung, die erstellt wird. Der Tag-Schlüssel wird als Tag: GuardDutyManaged angezeigt.

Using exclusion tag in selected instances

> **Note**
>
> Stellen Sie sicher, dass Sie Ihren Amazon EC2 EC2-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für Amazon EC2 aktiviert haben, wird jede EC2-Instance, die ohne Ausschluss-Tag gestartet wird, von der GuardDuty automatisierten Agentenkonfiguration abgedeckt.

Um den GuardDuty Security Agent für bestimmte Instances in Ihrem eigenständigen Konto zu konfigurieren

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie nicht überwachen und potenzielle Bedrohungen nicht erkennen GuardDuty möchten, das `false` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.
3. Gehen Sie wie folgt vor, damit die Ausschluss-Tags in den Instanz-Metadaten verfügbar sind:

   a. Sehen Sie sich auf dem Tab Details Ihrer Instance den Status für Tags zulassen in den Instanz-Metadaten an.

Wenn es derzeit Deaktiviert ist, gehen Sie wie folgt vor, um den Status auf Aktiviert zu ändern. Andernfalls überspringen Sie diesen Schritt.

b. Wählen Sie im Menü Aktionen die Option Instanzeinstellungen aus.

c. Wähle „Tags in Instanz-Metadaten zulassen“.

4. Nachdem Sie das Ausschluss-Tag hinzugefügt haben, führen Sie dieselben Schritte aus, wie auf der Registerkarte Für alle Instanzen konfigurieren angegeben.

Sie können jetzt die Laufzeit beurteilenDeckung für Amazon EC2 EC2-Instance.

Nur ausgewählte Mitgliedskonten

Configure for all instances

1. Wählen Sie auf der Seite Konten ein oder mehrere Konten aus, für die Sie die Runtime Monitoring-Automated Agent-Konfiguration (Amazon EC2) aktivieren möchten. Stellen Sie sicher, dass Runtime Monitoring für die Konten, die Sie in diesem Schritt auswählen, bereits aktiviert ist.
2. Wählen Sie unter Schutzpläne bearbeiten die entsprechende Option aus, um die Runtime Monitoring-Automated Agent-Konfiguration (Amazon EC2) zu aktivieren.
3. Wählen Sie Bestätigen aus.

Using inclusion tag in selected instances

Um den GuardDuty Security Agent für ausgewählte Instances zu konfigurieren

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `true` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.

   Durch Hinzufügen dieses Tags können Sie GuardDuty den Security Agent für Ihre markierten Amazon EC2 EC2-Instances verwalten. Sie müssen die automatische Agentenkonfiguration nicht explizit aktivieren (Runtime Monitoring — Automated Agent Configuration (EC2)).

Using exclusion tag in selected instances

> **Note**
>
> Stellen Sie sicher, dass Sie Ihren Amazon EC2 EC2-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für Amazon EC2 aktiviert haben, wird jede EC2-Instance, die ohne Ausschluss-Tag gestartet wird, von der GuardDuty automatisierten Agentenkonfiguration abgedeckt.

Um den GuardDuty Security Agent für ausgewählte Instances zu konfigurieren

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den EC2-Instances, die Sie nicht überwachen oder potenzielle Bedrohungen nicht erkennen GuardDuty möchten, das `false` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.
3. Gehen Sie wie folgt vor, damit die Ausschluss-Tags in den Instanz-Metadaten verfügbar sind:
   a. Sehen Sie sich auf dem Tab Details Ihrer Instance den Status für Tags zulassen in den Instanz-Metadaten an.

      Wenn es derzeit Deaktiviert ist, gehen Sie wie folgt vor, um den Status auf Aktiviert zu ändern. Andernfalls überspringen Sie diesen Schritt.
   b. Wählen Sie im Menü Aktionen die Option Instanzeinstellungen aus.
   c. Wähle „Tags in Instanz-Metadaten zulassen“.
4. Nachdem Sie das Ausschluss-Tag hinzugefügt haben, führen Sie dieselben Schritte aus, wie auf der Registerkarte Für alle Instanzen konfigurieren angegeben.

Sie können jetzt beurteilenDeckung für Amazon EC2 EC2-Instance.

Manuelles Verwalten des Security Agents für Amazon EC2 EC2-Instance

Nachdem Sie Runtime Monitoring aktiviert haben, müssen Sie den GuardDuty Security Agent manuell installieren. Durch die Installation des Agenten GuardDuty werden die Runtime-Ereignisse von den Amazon EC2 EC2-Instances empfangen.

Um den GuardDuty Security Agent zu verwalten, müssen Sie einen Amazon VPC-Endpunkt erstellen und dann die Schritte zur manuellen Installation des Security Agents befolgen.

Manuelles Erstellen eines Amazon VPC-Endpunkts

Bevor Sie den GuardDuty Security Agent installieren können, müssen Sie einen Amazon Virtual Private Cloud (Amazon VPC) -Endpunkt erstellen. Dies hilft beim GuardDuty Empfang der Runtime-Ereignisse Ihrer Amazon EC2 EC2-Instances.

> **Note**
>
> Für die Nutzung des VPC-Endpunkts fallen keine zusätzlichen Kosten an.

So erstellen Sie einen Amazon VPC-Endpunkt

1. Melden Sie sich bei der Amazon VPC-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPC Private Cloud die Option Endpoints aus.
3. Klicken Sie auf Endpunkt erstellen.
4. Wählen Sie auf der Seite Endpunkt erstellen für Servicekategorie die Option Andere Endpunkt-Services.
5. Geben Sie unter Servicename **`com.amazonaws.`*`us-east-1`*`.guardduty-data`** ein.

   Stellen Sie sicher, dass Sie *`us-east-1`* durch Ihr ersetzen. AWS-Region Dies muss dieselbe Region sein wie die Amazon EC2 EC2-Instance, die zu Ihrer AWS Konto-ID gehört.
6. Wählen Sie Service verifizieren.
7. Nachdem der Dienstname erfolgreich verifiziert wurde, wählen Sie die VPC aus, in der sich Ihre Instance befindet. Fügen Sie die folgende Richtlinie hinzu, um die Nutzung von Amazon VPC-Endpunkten nur auf das angegebene Konto zu beschränken. Unter Angabe der unter dieser Richtlinie angegebenen Organisations-`Condition` können Sie die folgende Richtlinie aktualisieren, um den Zugriff auf Ihren Endpunkt einzuschränken. Informationen zur Bereitstellung von Amazon VPC-Endpunktunterstützung für bestimmte Konto-IDs in Ihrer Organisation finden Sie unterOrganization condition to restrict access to your endpoint.

   ```
   {
    "Version": "2012-10-17",
    "Statement": [
   ```

```
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
 ]
}
```

Die `aws:PrincipalAccount`-Konto-ID muss mit dem Konto übereinstimmen, das die VPC und den VPC-Endpunkt enthält. Die folgende Liste zeigt, wie Sie den VPC-Endpunkt mit anderen AWS Konto-IDs teilen können:

- Um mehrere Konten für den Zugriff auf den VPC-Endpunkt anzugeben, `"aws:PrincipalAccount: "111122223333"` ersetzen Sie ihn durch den folgenden Block:

  ```
  "aws:PrincipalAccount": [
            "666666666666",
            "555555555555"
       ]
  ```

  Achten Sie darauf, die AWS Konto-IDs durch die Konto-IDs der Konten zu ersetzen, die auf den VPC-Endpunkt zugreifen müssen.

- Um allen Mitgliedern einer Organisation den Zugriff auf den VPC-Endpunkt zu ermöglichen, `"aws:PrincipalAccount: "111122223333"` ersetzen Sie ihn durch die folgende Zeile:

  ```
  "aws:PrincipalOrgID": "o-abcdef0123"
  ```

Achten Sie darauf, die Organisation *o-abcdef0123* durch Ihre Organisations-ID zu ersetzen.

- Um den Zugriff auf eine Ressource anhand einer Organisations-ID einzuschränken, fügen Sie Ihre zur Richtlinie hinzu. `ResourceOrgID` Weitere Informationen finden Sie unter `aws:ResourceOrgID` im IAM-Benutzerhandbuch.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. Wählen Sie unter Zusätzliche Einstellungen die Option DNS-Name aktivieren.
9. Wählen Sie unter Subnetze die Subnetze aus, in denen sich Ihre Instance befindet.
10. Wählen Sie unter Sicherheitsgruppen eine Sicherheitsgruppe aus, für die der eingehende Port 443 von Ihrer VPC (oder Ihrer Amazon EC2 EC2-Instance) aktiviert ist. Wenn Sie noch keine Sicherheitsgruppe haben, für die ein eingehender Port 443 aktiviert ist, finden Sie weitere Informationen unter Erstellen einer Sicherheitsgruppe im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

    Wenn bei der Einschränkung der eingehenden Berechtigungen für Ihre VPC (oder Instance) ein Problem auftritt, stellen Sie die Unterstützung für den eingehenden Port 443 von einer beliebigen IP-Adresse aus bereit. `(0.0.0.0/0)`

Manuelles Installieren des Security Agents

GuardDuty bietet die folgenden zwei Methoden zur Installation des GuardDuty Security Agents auf Ihren Amazon EC2 EC2-Instances:

- Methode 1 — Mithilfe AWS Systems Manager — Für diese Methode muss Ihre Amazon EC2 EC2-Instance AWS Systems Manager verwaltet werden.
- Methode 2 — Mithilfe von RPM-Installationsskripten — Sie können diese Methode unabhängig davon verwenden, ob Ihre Amazon EC2 EC2-Instances AWS Systems Manager verwaltet werden oder nicht.

Methode 1 — Durch die Verwendung von AWS Systems Manager

Um diese Methode zu verwenden, stellen Sie sicher, dass Ihre Amazon EC2 EC2-Instances AWS Systems Manager verwaltet werden, und installieren Sie dann den Agenten.

AWS Systems Manager verwaltete Amazon EC2 EC2-Instanz

Gehen Sie wie folgt vor, um Ihre Amazon EC2 EC2-Instances zu AWS Systems Manager verwalten.

- AWS Systems Managerhilft Ihnen bei der Verwaltung Ihrer AWS Anwendungen und Ressourcen end-to-end und ermöglicht sichere Abläufe in großem Maßstab.

  Informationen zur Verwaltung Ihrer Amazon EC2 EC2-Instances mit AWS Systems Manager finden Sie unter Systems Manager für Amazon EC2 EC2-Instances einrichten im AWS Systems Manager Benutzerhandbuch.
- Die folgende Tabelle zeigt die neuen GuardDuty verwalteten AWS Systems Manager Dokumente:

Dokumentname	Dokumenttyp	Zweck
`AmazonGuardDuty-RuntimeMonitoringSsmPlugin`	Distributor	Um den GuardDuty Security Agent zu verpacken.
`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`	Befehl	Um das Installations- und Deinstallationsskript auszuführen, um den Security Agent zu installieren. GuardDuty

  Weitere Informationen zu AWS Systems Manager finden Sie in den Amazon EC2 Systems Manager Manager-Dokumenten im AWS Systems Manager Benutzerhandbuch.

Um den GuardDuty Agenten für die Amazon EC2 EC2-Instance zu installieren, verwenden Sie AWS Systems Manager

1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich Dokumente
3. Wählen Sie unter Owned by Amazon die Option aus`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`.
4. Wählen Sie Run Command (Befehl ausführen) aus.

5. Geben Sie die folgenden Run-Command-Parameter ein

   - Aktion: Wählen Sie Installieren.
   - Installationstyp: Wählen Sie Installieren oder Deinstallieren.
   - Name: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`
   - Version: Wenn dieses Feld leer bleibt, erhalten Sie die neueste Version des GuardDuty Security Agents. Weitere Informationen zu den Release-Versionen finden Sie unterGuardDuty Sicherheitsagent für Amazon EC2 EC2-Instances.

6. Wählen Sie die Amazon EC2 EC2-Zielinstanz aus. Sie können eine oder mehrere Amazon EC2 EC2-Instances auswählen. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Befehle von der Konsole aus AWS Systems Manager ausführen
7. Überprüfen Sie, ob die GuardDuty Agenteninstallation fehlerfrei ist. Weitere Informationen finden Sie unter Der Installationsstatus des GuardDuty Security Agents wird überprüft.

Methode 2 — Mithilfe von RPM-Installationsskripten

> **Important**
>
> Wir empfehlen dringend, die RPM-Signatur des GuardDuty Security Agents zu überprüfen, bevor Sie ihn auf Ihrem Computer installieren.

1. Überprüfen Sie die GuardDuty RPM-Signatur des Security Agents

   a. Laden Sie den entsprechenden öffentlichen Schlüssel, die Signatur von x86_64 RPM, die Signatur von arm64 RPM und den entsprechenden Zugriffslink zu den RPM-Skripten herunter, die in Amazon S3 S3-Buckets gehostet werden

      Sie können die folgenden Vorlagen verwenden, um den öffentlichen Schlüssel, die Signatur von x86_64 RPM, die Signatur von arm64 RPM und den entsprechenden Zugriffslink zu den RPM-Skripten zu erstellen. Ersetzen Sie den Wert von AWS-Region, der AWS Konto-ID und der GuardDuty Agentenversion, um auf die RPM-Skripts zuzugreifen.

      - Öffentlicher Schlüssel:

        ```
        s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/publickey.pem
        ```

- GuardDuty RPM-Signatur des Security Agents:

  Signatur von x86_64 RPM

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/
  amazon-guardduty-agent-1.1.0.x86_64.sig
  ```

  Signatur von arm64 RPM

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/
  amazon-guardduty-agent-1.1.0.arm64.sig
  ```

- Greifen Sie auf Links zu den RPM-Skripten im Amazon S3 S3-Bucket zu:

  Zugangslink für x86_64 RPM

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/
  amazon-guardduty-agent-1.1.0.x86_64.rpm
  ```

  Zugangslink für arm64 RPM

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/
  amazon-guardduty-agent-1.1.0.arm64.rpm
  ```

Stellen Sie sicher, dass Sie im folgenden Befehl zum Herunterladen des entsprechenden öffentlichen Schlüssels, der Signatur von x86_64 RPM, der Signatur von arm64 RPM und des entsprechenden Zugriffs-Links zu den RPM-Skripten, die in Amazon S3 S3-Buckets gehostet werden, die Konto-ID durch die entsprechende AWS-Konto ID und die Region durch Ihre aktuelle Region ersetzen.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
x86_64/amazon-guardduty-agent-1.1.0.x86_64.rpm ./amazon-guardduty-
agent-1.1.0.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
x86_64/amazon-guardduty-agent-1.1.0.x86_64.sig ./amazon-guardduty-
agent-1.1.0.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
publickey.pem ./publickey.pem
```

AWS-Region	Name der Region	AWS Konto-ID
eu-west-1	Europa (Irland)	694911143906
us-east-1	USA Ost (Nord-Virginia)	593207742271
us-west-2	USA West (Oregon)	733349766148
eu-west-3	Europa (Paris)	665651866788
us-east-2	USA Ost (Ohio)	307168627858
eu-central-1	Europa (Frankfurt)	323658145986
ap-northeast-2	Asien-Pazifik (Seoul)	914738172881
eu-north-1	Europa (Stockholm)	591436053604
ap-east-1	Asien-Pazifik (Hongkong)	258348409381
me-south-1	Naher Osten (Bahrain)	536382113932
eu-west-2	Europa (London)	892757235363
ap-northeast-1	Asien-Pazifik (Tokio)	533107202818
ap-southeast-1	Asien-Pazifik (Singapur)	174946120834
ap-south-1	Asien-Pazifik (Mumbai)	251508486986
ap-southeast-3	Asien-Pazifik (Jakarta)	510637619217
sa-east-1	Südamerika (São Paulo)	758426053663
ap-northeast-3	Asien-Pazifik (Osaka)	273192626886
eu-south-1	Europa (Milan)	266869475730
af-south-1	Afrika (Kapstadt)	197869348890
ap-southeast-2	Asien-Pazifik (Sydney)	005257825471

me-central-1	Naher Osten (VAE)	000014521398
us-west-1	USA West (Nordkalifornien)	684579721401
ca-central-1	Kanada (Zentral)	354763396469
ap-south-2	Asien-Pazifik (Hyderabad)	950823858135
eu-south-2	Europa (Spain)	919611009337
eu-central-2	Europa (Zürich)	529164026651
ap-southeast-4	Asien-Pazifik (Melbourne)	251357961535
il-central-1	Israel (Tel Aviv)	870907303882

b. Importiert den öffentlichen Schlüssel in die Datenbank

```
gpg --import publickey.pem
```

gpg zeigt, dass der Import erfolgreich war

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

c. Verifiziere die Signatur

```
gpg --verify amazon-guardduty-agent-1.1.0.x86_64.sig amazon-guardduty-
agent-1.1.0.x86_64.rpm
```

Wenn die Überprüfung erfolgreich ist, wird eine Meldung ähnlich dem folgenden Ergebnis angezeigt. Sie können jetzt mit der Installation des GuardDuty Security Agents mithilfe von RPM fortfahren.

Beispielausgabe:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
```

```
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

Wenn die Überprüfung fehlschlägt, bedeutet dies, dass die Signatur auf RPM möglicherweise manipuliert wurde. Sie müssen den öffentlichen Schlüssel aus der Datenbank entfernen und den Überprüfungsprozess erneut versuchen.

Beispiel:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

d. Entfernen Sie den öffentlichen Schlüssel aus der Datenbank.

```
gpg --delete-keys AwsGuardDuty
```

2. Stellen Sie von Linux oder macOS aus eine Connect mit SSH her.
3. Installieren Sie den GuardDuty Security Agent mit dem folgenden Befehl:

```
sudo rpm -ivh amazon-guardduty-agent-1.1.0.x86_64.rpm
```

4. Überprüfen Sie, ob die GuardDuty Agent-Installation fehlerfrei ist. Weitere Informationen zu den Schritten finden Sie unterDer Installationsstatus des GuardDuty Security Agents wird überprüft.
5. (Optional) entfernen Sie den GuardDuty Security Agent mithilfe des folgenden Befehls:

```
sudo rpm -ev amazon-guardduty-agent
```

Fehler: Nicht genügend Arbeitsspeicher

Wenn bei der manuellen Installation oder Aktualisierung des GuardDuty Security Agents für Amazon EC2 ein `out-of-memory` Fehler auftritt, finden Sie weitere Informationen unterBehebung eines Fehlers wegen unzureichenden Speichers.

Der Installationsstatus des GuardDuty Security Agents wird überprüft

Um zu überprüfen, ob der GuardDuty Security Agent fehlerfrei ist

1. Stellen Sie von Linux oder macOS aus eine Connect mit SSH her.
2. Führen Sie den folgenden Befehl aus, um den Status des GuardDuty Security Agents zu überprüfen:

```
sudo systemctl status amazon-guardduty-agent
```

Wenn Sie die Installationsprotokolle des Security Agents einsehen möchten, finden Sie sie unter/var/log/amzn-guardduty-agent/.

Um die Protokolle einzusehen, tun Sie diessudo journalctl -u amazon-guardduty-agent.

Den GuardDuty Security Agent manuell aktualisieren

Sie können den GuardDuty Security Agent mit dem Befehl Ausführen aktualisieren. Sie können dieselben Schritte ausführen, die Sie bei der Installation des GuardDuty Security Agents verwendet haben.

Den Security Agent manuell deinstallieren

In diesem Abschnitt finden Sie Methoden zur Deinstallation des GuardDuty Security Agents von Ihren Amazon EC2 EC2-Ressourcen. Wenn Sie außerdem planen, Runtime Monitoring zu deaktivieren, finden Sie weitere Informationen unterAuswirkungen der Deaktivierung.

Methode 1 — Mit dem Befehl Run

So deinstallieren Sie den GuardDuty Security Agent mit dem Befehl Run

1. Sie können den GuardDuty Security Agent deinstallieren, indem Sie die im AWS Systems Manager Benutzerhandbuch AWS Systems Manager unter Befehl ausführen angegebenen Schritte ausführen ausführen. Verwenden Sie die Aktion Deinstallieren in den Parametern, um den GuardDuty Security Agent zu deinstallieren.

   Stellen Sie im Abschnitt Ziele sicher, dass sich die Auswirkungen nur auf die Amazon EC2 EC2-Instances auswirken, von denen Sie den Security Agent deinstallieren möchten.

   Verwenden Sie das folgende GuardDuty Dokument und den folgenden Vertriebspartner:

   - Name des Dokuments: AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin
   - Vertriebspartner: AmazonGuardDuty-RuntimeMonitoringSsmPlugin
2. Nachdem Sie alle Details angegeben haben und Ausführen wählen, wird der Security Agent, den er auf den Ziel-Instances von Amazon EC2 installiert hat, entfernt.

Um die Amazon VPC-Endpunktkonfiguration zu entfernen, müssen Sie sowohl Runtime Monitoring als auch Amazon EKS Runtime Monitoring deaktivieren.

Methode 2 — Mithilfe des RPM-Skripts

Um den GuardDuty Security Agent mit dem RPM zu deinstallieren

1. Stellen Sie von Linux oder macOS aus eine Connect mit SSH her.
2. Mit dem folgenden Befehl wird der GuardDuty Security Agent von der Amazon EC2 EC2-Instance deinstalliert, zu der Sie eine Verbindung herstellen:

```
sudo rpm -e amazon-guardduty-agent
```

Sie können auch die mit diesem Befehl verknüpften Protokolle überprüfen.

Löschen Sie den Amazon VPC-Endpunkt

Wenn Sie Runtime Monitoring deaktivieren oder den GuardDuty Security Agent für Ihr Konto deinstallieren möchten, können Sie auch den manuell erstellten Amazon VPC-Endpunkt löschen (Manuelles Erstellen eines Amazon VPC-Endpunkts).

So löschen Sie den Amazon VPC-Endpunkt mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den Endpunkt aus, der zum Zeitpunkt der Aktivierung von Runtime Monitoring manuell erstellt wurde.
4. Wählen Sie Actions (Aktionen), Delete VPC Endpoint (VPC-Endpunkte löschen).
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein.
6. Wählen Sie Löschen.

Um den Amazon VPC-Endpunkt zu löschen, verwenden Sie AWS CLI

- delete-vpc-endpoints (AWS Command Line Interface)
- Remove-EC2VpcEndpointCmdlet (Tools für Windows) PowerShell

Verwaltung eines automatisierten Sicherheitsagenten für Fargate (nur Amazon ECS)

GuardDuty Agent für ein eigenständiges Konto konfigurieren

Derzeit unterstützt Runtime Monitoring die Verwaltung des Security Agents für Ihre Amazon ECS-Cluster (AWS Fargate) nur über GuardDuty. Die manuelle Verwaltung des Security Agents auf Amazon ECS-Clustern wird nicht unterstützt.

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Gehen Sie auf der Registerkarte Konfiguration wie folgt vor:

   a. Zur Verwaltung der automatisierten Agentenkonfiguration für alle Amazon ECS-Cluster (Kontoebene)

      Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration für AWS Fargate (nur ECS) die Option Aktivieren aus. Wenn eine neue Fargate Amazon ECS-Task gestartet GuardDuty wird, wird die Bereitstellung des Sicherheitsagenten verwaltet.

      - Wählen Sie Speichern.

   b. Verwaltung der automatisierten Agentenkonfiguration durch Ausschluss einiger Amazon ECS-Cluster (Cluster-Ebene)

      i. Fügen Sie dem Amazon ECS-Cluster, für den Sie alle Aufgaben ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged` `false`

      ii. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
```

```
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
```

```
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

iii. Wählen Sie auf der Registerkarte Konfiguration im Abschnitt Automatisierte Agentenkonfiguration die Option Aktivieren aus.

> **Note**
>
> Fügen Sie Ihrem Amazon ECS-Cluster immer das Ausschluss-Tag hinzu, bevor Sie die automatische GuardDuty Agentenverwaltung für Ihr Konto aktivieren. Andernfalls wird der Security Agent bei allen Aufgaben eingesetzt, die innerhalb des entsprechenden Amazon ECS-Clusters gestartet werden.

Für die Amazon ECS-Cluster, die nicht ausgeschlossen wurden, GuardDuty wird die Bereitstellung des Security Agents im Sidecar-Container verwaltet.

iv. Wählen Sie Speichern.

c. Verwaltung der automatisierten Agentenkonfiguration durch Einbeziehung einiger Amazon ECS-Cluster (Cluster-Ebene)

i. Fügen Sie einem Amazon ECS-Cluster, für den Sie alle Aufgaben einbeziehen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged` `true`

ii. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
```

```
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

Konfiguration des GuardDuty Agenten für eine Umgebung mit mehreren Konten

In einer Umgebung mit mehreren Konten kann nur das delegierte GuardDuty Administratorkonto die automatische Agentenkonfiguration für die Mitgliedskonten aktivieren oder deaktivieren und die automatische Agentenkonfiguration für Amazon ECS-Cluster verwalten, die zu den Mitgliedskonten in ihrer Organisation gehören. Ein GuardDuty Mitgliedskonto kann diese Konfiguration nicht ändern. Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten in. GuardDuty

Aktivierung der automatisierten Agentenkonfiguration für ein delegiertes Administratorkonto GuardDuty

Manage for all Amazon ECS clusters (account level)

Wenn Sie für Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben, stehen Ihnen die folgenden Optionen zur Verfügung:

- Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus. GuardDuty wird den Security Agent für alle Amazon ECS-Aufgaben bereitstellen und verwalten, die gestartet werden.
- Wählen Sie Konten manuell konfigurieren.

Wenn Sie im Bereich Runtime Monitoring die Option Konten manuell konfigurieren ausgewählt haben, gehen Sie wie folgt vor:

1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Konten manuell konfigurieren aus.
2. Wählen Sie im Abschnitt Delegiertes GuardDuty Administratorkonto (dieses Konto) die Option Aktivieren aus.

Wählen Sie Speichern.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Fügen Sie diesem Amazon ECS-Cluster ein Tag mit dem Schlüssel-Wert-Paar als `GuardDutyManaged` - hinzu. `false`
2. Verhindern Sie die Änderung von Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte

Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
5.

> **Note**
>
> Fügen Sie Ihren Amazon ECS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Sidecar-Container an alle Container in den Amazon ECS-Aufgaben angehängt, die gestartet werden.

Wählen Sie auf der Registerkarte Konfiguration in der automatisierten Agentenkonfiguration die Option Aktivieren aus.

Für die Amazon ECS-Cluster, die nicht ausgeschlossen wurden, GuardDuty wird die Bereitstellung des Security Agents im Sidecar-Container verwaltet.

6. Wählen Sie Speichern.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Fügen Sie einem Amazon ECS-Cluster, für den Sie alle Aufgaben einbeziehen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged` `true`
2. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
```

```
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
```

```
            }
        }
    ]
}
```

> **Note**
>
> Wenn Sie Inclusion-Tags für Ihre Amazon ECS-Cluster verwenden, müssen Sie den GuardDuty Agenten nicht explizit über die automatische Agentenkonfiguration aktivieren.

Automatische Aktivierung für alle Mitgliedskonten

Manage for all Amazon ECS clusters (account level)

Bei den folgenden Schritten wird davon ausgegangen, dass Sie im Abschnitt Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben.

1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus. GuardDuty wird den Security Agent für alle Amazon ECS-Aufgaben bereitstellen und verwalten, die gestartet werden.
2. Wählen Sie Speichern.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Fügen Sie diesem Amazon ECS-Cluster ein Tag mit dem Schlüssel-Wert-Paar als `GuardDutyManaged` - hinzu. `false`
2. Verhindern Sie die Änderung von Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
```

```
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
```

```
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
5.

> **Note**
>
> Fügen Sie Ihren Amazon ECS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Sidecar-Container an alle Container in den Amazon ECS-Aufgaben angehängt, die gestartet werden.

   Wählen Sie auf der Registerkarte Konfiguration die Option Bearbeiten aus.
6. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus

   Für die Amazon ECS-Cluster, die nicht ausgeschlossen wurden, GuardDuty wird die Bereitstellung des Security Agents im Sidecar-Container verwaltet.
7. Wählen Sie Speichern.

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Unabhängig davon, wie Sie Runtime Monitoring aktivieren, helfen Ihnen die folgenden Schritte dabei, ausgewählte Amazon ECS Fargate-Aufgaben für alle Mitgliedskonten in Ihrer Organisation zu überwachen.

1. Aktivieren Sie im Abschnitt Automatisierte Agentenkonfiguration keine Konfiguration. Behalten Sie die Runtime Monitoring-Konfiguration bei, die Sie im vorherigen Schritt ausgewählt haben.
2. Wählen Sie Speichern.
3. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
```

```
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
```

```
}
```

> **Note**
>
> Wenn Sie Inclusion-Tags für Ihre Amazon ECS-Cluster verwenden, müssen Sie die automatische Verwaltung der GuardDuty Agenten nicht explizit aktivieren.

Aktivierung der automatisierten Agentenkonfiguration für bestehende aktive Mitgliedskonten

Manage for all Amazon ECS clusters (account level)

1. Auf der Seite Runtime Monitoring können Sie auf der Registerkarte Konfiguration den aktuellen Status der automatisierten Agentenkonfiguration einsehen.
2. Wählen Sie im Bereich Automatisierte Agentenkonfiguration im Abschnitt Aktive Mitgliedskonten die Option Aktionen aus.
3. Wählen Sie bei Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
4. Wählen Sie Bestätigen aus.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Fügen Sie diesem Amazon ECS-Cluster ein Tag mit dem Schlüssel-Wert-Paar als `GuardDutyManaged` - hinzu. `false`
2. Verhindern Sie die Änderung von Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
```

```
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
```

```
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
5.

> **Note**
>
> Fügen Sie Ihren Amazon ECS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Sidecar-Container an alle Container in den Amazon ECS-Aufgaben angehängt, die gestartet werden.

   Wählen Sie auf der Registerkarte Konfiguration im Abschnitt Automatisierte Agentenkonfiguration unter Aktive Mitgliedskonten die Option Aktionen aus.
6. Wählen Sie bei Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.

   Für die Amazon ECS-Cluster, die nicht ausgeschlossen wurden, GuardDuty wird die Bereitstellung des Security Agents im Sidecar-Container verwaltet.
7. Wählen Sie Bestätigen aus.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Fügen Sie einem Amazon ECS-Cluster, für den Sie alle Aufgaben einbeziehen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged` `true`
2. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
```

```
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Wenn Sie Inclusion-Tags für Ihre Amazon ECS-Cluster verwenden, müssen Sie die automatische Agentenkonfiguration nicht explizit aktivieren.

Automatische Aktivierung der automatischen Agentenkonfiguration für neue Mitglieder

Manage for all Amazon ECS clusters (account level)

1. Wählen Sie auf der Seite Runtime Monitoring die Option Bearbeiten aus, um die bestehende Konfiguration zu aktualisieren.
2. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Automatisch für neue Mitgliedskonten aktivieren aus.
3. Wählen Sie Speichern.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Fügen Sie diesem Amazon ECS-Cluster ein Tag mit dem Schlüssel-Wert-Paar als `GuardDutyManaged` - hinzu. `false`
2. Verhindern Sie die Änderung von Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
```

```
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
```

```
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
5.

> **Note**
>
> Fügen Sie Ihren Amazon ECS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Sidecar-Container an alle Container in den Amazon ECS-Aufgaben angehängt, die gestartet werden.

   Wählen Sie auf der Registerkarte Konfiguration im Abschnitt Automatisierte Agentenkonfiguration die Option Automatisch für neue Mitgliedskonten aktivieren aus.

   Für die Amazon ECS-Cluster, die nicht ausgeschlossen wurden, GuardDuty wird die Bereitstellung des Security Agents im Sidecar-Container verwaltet.
6. Wählen Sie Speichern.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Fügen Sie einem Amazon ECS-Cluster, für den Sie alle Aufgaben einbeziehen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged` `true`
2. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte

Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Wenn Sie Inclusion-Tags für Ihre Amazon ECS-Cluster verwenden, müssen Sie die automatische Agentenkonfiguration nicht explizit aktivieren.

Selektives Aktivieren der automatisierten Agentenkonfiguration für aktive Mitgliedskonten

Manage for all Amazon ECS (account level)

1. Wählen Sie auf der Seite Konten die Konten aus, für die Sie die Runtime Monitoring-Automated Agent-Konfiguration (ECS-Fargate) aktivieren möchten. Sie können mehrere Konten auswählen. Stellen Sie sicher, dass die Konten, die Sie in diesem Schritt auswählen, bereits für Runtime Monitoring aktiviert sind.
2. Wählen Sie unter Schutzpläne bearbeiten die entsprechende Option aus, um die Runtime Monitoring-Automated Agent-Konfiguration (ECS-Fargate) zu aktivieren.
3. Wählen Sie Bestätigen aus.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Fügen Sie diesem Amazon ECS-Cluster ein Tag mit dem Schlüssel-Wert-Paar als `GuardDutyManaged` - hinzu. `false`
2. Verhindern Sie die Änderung von Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
```

```
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
```

```
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
5.

> **Note**
>
> Fügen Sie Ihren Amazon ECS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische GuardDuty Agentenverwaltung für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Sidecar-Container an alle Container in den Amazon ECS-Aufgaben angehängt, die gestartet werden.

   Wählen Sie auf der Seite Konten die Konten aus, für die Sie die Runtime Monitoring-Automated Agent-Konfiguration (ECS-Fargate) aktivieren möchten. Sie können mehrere Konten auswählen. Stellen Sie sicher, dass die Konten, die Sie in diesem Schritt auswählen, bereits für Runtime Monitoring aktiviert sind.

   Für die Amazon ECS-Cluster, die nicht ausgeschlossen wurden, GuardDuty wird die Bereitstellung des Security Agents im Sidecar-Container verwaltet.
6. Wählen Sie unter Schutzpläne bearbeiten die entsprechende Option aus, um die Runtime Monitoring-Automated Agent-Konfiguration (ECS-Fargate) zu aktivieren.
7. Wählen Sie Speichern.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Stellen Sie sicher, dass Sie die automatische Agentenkonfiguration (oder Runtime Monitoring-Automated Agent-Konfiguration (ECS-Fargate)) nicht für die ausgewählten Konten aktivieren, die über die Amazon ECS-Cluster verfügen, die Sie überwachen möchten.
2. Fügen Sie einem Amazon ECS-Cluster, für den Sie alle Aufgaben einbeziehen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged` `true`

3. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Wenn Sie Inclusion-Tags für Ihre Amazon ECS-Cluster verwenden, müssen Sie die automatische Agentenkonfiguration nicht explizit aktivieren.

Automatisches Verwalten des Security Agents für Amazon EKS-Cluster

Konfiguration des automatisierten Agenten für ein eigenständiges Konto

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Wählen Sie auf der Registerkarte Konfiguration die Option Aktivieren aus, um die automatische Agentenkonfiguration für Ihr Konto zu aktivieren.

Bevorzugter Ansatz für die Installation des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Alle EKS-Cluster überwachen)	1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Aktivieren aus. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle vorhandenen und potenziell neuen EKS-Cluster in Ihrem Konto. 2. Wählen Sie Speichern.
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft. Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent nicht auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch.

Bevorzugter Ansatz für die Installation des GuardDuty Security Agents	Schritte
	2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Öffnen Sie die Konsole unter https://console.aws.amazon.com/guardduty/ GuardDuty . 4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.

Bevorzugter Ansatz für die Installation des GuardDuty Security Agents	Schritte
	> **Note** > Fügen Sie Ihren EKS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische GuardDuty Agentenverwaltung für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto bereitgestellt. 5. Wählen Sie auf der Registerkarte Konfiguration im Bereich GuardDuty Agentenverwaltung die Option Aktivieren aus. Für die EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden, GuardDuty wird die Bereitstellung und Aktualisierung des GuardDuty Security Agents verwaltet. 6. Wählen Sie Speichern. Um einen EKS-Cluster von der Überwachung auszuschließen, nachdem der GuardDuty Security Agent bereits auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch.

Bevorzugter Ansatz für die Installation des GuardDuty Security Agents	Schritte
	Nach diesem Schritt GuardDuty wird der Security Agent für diesen Cluster nicht aktualisiert. Der Security Agent bleibt jedoch weiterhin installiert und empfängt GuardDuty weiterhin die Runtime-E reignisse von diesem EKS-Cluster. Dies kann sich auf Ihre Nutzungsstatistiken auswirken. 2. Um zu verhindern, dass Tags, außer durch vertrauen swürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:`

Bevorzugter Ansatz für die Installation des GuardDuty Security Agents	Schritte

	<pre>iam::123456789012:role/org-admins/ia
	m-admin"]</pre>
	3. Um die Laufzeit-Ereignisse von diesem Cluster nicht mehr zu empfangen, müssen Sie den bereitgestellten Sicherheitsagent aus diesem EKS-Cluster entfernen. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie unter Auswirkungen der Deaktivierung und Bereinigung von Ressourcen.

Bevorzugter Ansatz für die Installation des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster mithilfe von Einschließen-Tags überwachen	1. Stellen Sie sicher, dass Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Deaktivieren auswählen. Lassen Sie Runtime Monitoring aktiviert. 2. Wählen Sie Speichern. 3. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `true` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. GuardDuty verwaltet die Verteilung und Aktualisierung des Security Agents für die ausgewählten EKS-Cluster, die Sie überwachen möchten. 4. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität.

Bevorzugter Ansatz für die Installation des GuardDuty Security Agents	Schritte
	Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Den Agent manuell verwalten	1. Stellen Sie sicher, dass Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Deaktivieren auswählen. Lassen Sie Runtime Monitoring aktiviert. 2. Wählen Sie Speichern. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster.

Konfiguration eines automatisierten Agenten für Umgebungen mit mehreren Konten

In Umgebungen mit mehreren Konten kann nur das delegierte GuardDuty Administratorkonto die automatische Agentenkonfiguration für die Mitgliedskonten aktivieren oder deaktivieren und den automatisierten Agenten für die EKS-Cluster verwalten, die zu den Mitgliedskonten in ihrer Organisation gehören. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten.

Konfiguration der automatisierten Agentenkonfiguration für das delegierte Administratorkonto GuardDuty

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Alle EKS-Cluster überwachen)	Wenn Sie im Bereich Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben, stehen Ihnen die folgenden Optionen zur Verfügung: • Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus. GuardDuty verteilt und verwaltet den Security Agent für alle EKS-Cluster, die zum delegierten GuardDuty Administratorkonto gehören, sowie für alle EKS-Cluster, die zu allen bestehenden und potenziell neuen Mitgliedskonten in der Organisation gehören. • Wählen Sie Konten manuell konfigurieren. Wenn Sie im Bereich Runtime Monitoring die Option Konten manuell konfigurieren ausgewählt haben, gehen Sie wie folgt vor: 1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Konten manuell konfigurieren aus. 2. Wählen Sie im Abschnitt Delegiertes GuardDuty Administr atorkonto (dieses Konto) die Option Aktivieren aus. Wählen Sie Speichern.
Alle EKS-Cluster überwachen, jedoch einige davon ausschlie ßen (mithilfe des Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Um einen EKS-Cluster von der Überwachung auszuschließen, obwohl der GuardDuty Security Agent nicht auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::1234`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte

```
56789012:role/org-admins/iam-admin", "arn:aws:
iam::123456789012:role/org-admins/iam-admin"]
```

3. Öffnen Sie die Konsole unter https://console.aws.amazon.com/guardduty/ GuardDuty .
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.

> **Note**
>
> Fügen Sie Ihren EKS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische GuardDuty Agentenverwaltung für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto bereitgestellt.

5. Wählen Sie auf der Registerkarte Konfiguration im Bereich GuardDuty Agentenverwaltung die Option Aktivieren aus.

   Für die EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden, GuardDuty wird die Bereitstellung und Aktualisierung des GuardDuty Security Agents verwaltet.
6. Wählen Sie Speichern.

Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent auf diesem Cluster installiert wurde

1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu.

   Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Wenn Sie den Automated Agent für diesen EKS-Cluster aktiviert hatten, GuardDuty wird der Security Agent für diesen Cluster nach diesem Schritt nicht aktualisiert. Der Security Agent bleibt jedoch weiterhin installiert und empfängt GuardDuty weiterhin die Runtime-Ereignisse von diesem EKS-Cluster. Dies kann sich auf Ihre Nutzungsstatistiken auswirken.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Um die Laufzeit-Ereignisse von diesem Cluster nicht mehr zu empfangen, müssen Sie den bereitgestellten Sicherheitsagent aus diesem EKS-Cluster entfernen. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie unter Auswirkungen der Deaktivierung und Bereinigung von Ressourcen 4. Wenn Sie den GuardDuty Security Agent für diesen EKS-Clust er manuell verwaltet haben, finden Sie weitere Informationen unterAuswirkungen der Deaktivierung und Bereinigung von Ressourcen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster mithilfe von Einschließen-Tags überwachen	Unabhängig davon, wie Sie Runtime Monitoring aktiviert haben, helfen Ihnen die folgenden Schritte bei der Überwachung ausgewählter EKS-Cluster in Ihrem Konto: 1. Stellen Sie sicher, dass Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für delegiertes GuardDuty Administratorkonto (dieses Konto) deaktivieren auswählen. Behalten Sie die Runtime Monitoring-Konfiguration bei, die Sie im vorherigen Schritt konfiguriert haben. 2. Wählen Sie Speichern. 3. Fügen Sie Ihrem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `true` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. GuardDuty verwaltet die Verteilung und Aktualisierung des Security Agents für die ausgewählten EKS-Cluster, die Sie überwachen möchten. 4. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen Sie *access-project* durch `GuardDuty Managed` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Verwalten Sie den Security Agent manuell GuardDuty	Unabhängig davon, wie Sie Runtime Monitoring aktiviert haben, können Sie den Security Agent für Ihre EKS-Cluster manuell verwalten. 1. Stellen Sie sicher, dass Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für delegiertes GuardDuty Administratorkonto (dieses Konto) deaktivieren auswählen. Behalten Sie die Runtime Monitoring-Konfiguration bei, die Sie im vorherigen Schritt konfiguriert haben. 2. Wählen Sie Speichern. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster.

Automatischer Agent für alle Mitgliedskonten automatisch aktivieren

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Alle EKS-Cluster überwachen)	In diesem Thema geht es darum, Runtime Monitoring für alle Mitgliedskonten zu aktivieren. Daher wird bei den folgenden Schritten davon ausgegangen, dass Sie im Abschnitt Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben. 1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus. GuardDuty verteilt und verwaltet den Security Agent für alle EKS-Cluster, die zum delegierten GuardDuty Administratorkonto gehören, sowie für alle EKS-Cluster, die zu allen bestehenden und potenziell neuen Mitgliedskonten in der Organisation gehören. 2. Wählen Sie Speichern.
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft. Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent nicht auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Öffnen Sie die Konsole unter https://console.aws.amazon.com/guardduty/ GuardDuty . 4. Wählen Sie im Navigationsbereich Runtime Monitoring aus. **Note** Fügen Sie Ihren EKS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie Automated Agent für Ihr Konto

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto installiert. 5. Wählen Sie auf der Registerkarte Konfiguration im Abschnitt Runtime Monitoring-Konfiguration die Option Bearbeiten aus. 6. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus. Für die EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden, GuardDuty wird die Bereitstellung und Aktualisierung des GuardDuty Security Agents verwaltet. 7. Wählen Sie Speichern. Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. 2. Wenn Sie die automatische Agentenkonfiguration für diesen EKS-Cluster aktiviert hatten, GuardDuty wird der Security Agent für diesen Cluster nach diesem Schritt nicht aktualisiert. Der Security Agent bleibt jedoch weiterhin installiert und empfängt GuardDuty weiterhin die Runtime-Ereignisse von diesem EKS-Cluster. Dies kann sich auf Ihre Nutzungsstatistiken auswirken. Um die Laufzeit-Ereignisse von diesem Cluster nicht mehr zu empfangen, müssen Sie den bereitgestellten Sicherheitsagent aus diesem EKS-Cluster entfernen. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	unter Auswirkungen der Deaktivierung und Bereinigung von Ressourcen 3. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDuty Managed` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 4. Wenn Sie den GuardDuty Security Agent für diesen EKS-Cluster manuell verwaltet haben, finden Sie weitere Informationen unter. Auswirkungen der Deaktivierung und Bereinigung von Ressourcen

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster mithilfe von Einschließen-Tags überwachen	Unabhängig davon, wie Sie Runtime Monitoring aktiviert haben, helfen Ihnen die folgenden Schritte bei der Überwachung ausgewählter EKS-Cluster für alle Mitgliedskonten in Ihrer Organisation: 1. Aktivieren Sie im Abschnitt Automatisierte Agentenkonfiguration keine Konfiguration. Behalten Sie die Konfiguration für Runtime Monitoring mit der Konfiguration im vorherigen Schritt bei. 2. Wählen Sie Speichern. 3. Fügen Sie Ihrem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `true` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. GuardDuty verwaltet die Verteilung und Aktualisierung des Security Agents für die ausgewählten EKS-Cluster, die Sie überwachen möchten. 4. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *`ec2: CreateTags`* durch `eks:TagResource` . • Ersetzen Sie *`ec2: DeleteTags`* durch. `eks:UntagResource` • Ersetzen Sie *`access-project`* durch `GuardDutyManaged` .

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Verwalten Sie den Security Agent manuell GuardDuty	Unabhängig davon, wie Sie Runtime Monitoring aktiviert haben, können Sie den Security Agent für Ihre EKS-Cluster manuell verwalten. 1. Aktivieren Sie im Abschnitt Automatisierte Agentenkonfiguration keine Konfiguration. Behalten Sie die Konfiguration für Runtime Monitoring mit der Konfiguration im vorherigen Schritt bei. 2. Wählen Sie Speichern. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster.

Aktivierung des automatisierten Agenten für alle vorhandenen aktiven Mitgliedskonten

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Um den GuardDuty Security Agent für bestehende aktive Mitgliedskonten in Ihrem Unternehmen zu verwalten

- GuardDuty Um Runtime-Ereignisse von den EKS-Clustern zu empfangen, die zu den bestehenden aktiven Mitgliedskonten in der Organisation gehören, müssen Sie einen bevorzugten Ansatz für die Verwaltung des GuardDuty Security Agents für diese EKS-Cluster wählen. Weitere Informationen zu diesen Ansätzen finden Sie unter Methoden zur Verwaltung des GuardDuty Security Agents.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Alle EKS-Cluster überwachen)	So überwachen Sie alle EKS-Cluster auf allen vorhanden en aktiven Mitgliedskonten 1. Auf der Seite Runtime Monitoring können Sie auf der Registerkarte Konfiguration den aktuellen Status der automatisierten Agentenkonfiguration einsehen. 2. Wählen Sie im Bereich Automatisierte Agentenko nfiguration im Abschnitt Aktive Mitgliedskonten die Option Aktionen aus. 3. Wählen Sie bei Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten. 4. Wählen Sie Bestätigen aus.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft. Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent nicht auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *`ec2: CreateTags`* durch `eks:TagResource`. • Ersetzen Sie *`ec2: DeleteTags`* durch `eks:UntagResource` • Ersetzen Sie *`access-project`* durch `GuardDutyManaged`. • Ersetzen Sie *`123456789012`* durch die AWS-Konto ID der vertrauenswürdigen Entität.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Öffnen Sie die Konsole unter https://console.aws.amazon.com/guardduty/ GuardDuty . 4. Wählen Sie im Navigationsbereich Runtime Monitoring aus. **Note** Fügen Sie Ihren EKS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto installiert. 5. Wählen Sie auf der Registerkarte Konfiguration im Bereich Automatisierte Agentenkonfiguration unter Aktive Mitgliedskonten die Option Aktionen aus. 6. Wählen Sie bei Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten. 7. Wählen Sie Bestätigen aus.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Um einen EKS-Cluster von der Überwachung auszuschl ießen, nachdem der GuardDuty Security Agent bereits auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutze rhandbuch. Nach diesem Schritt GuardDuty wird der Security Agent für diesen Cluster nicht aktualisiert. Der Security Agent bleibt jedoch weiterhin installiert und empfängt GuardDuty weiterhin die Runtime-E reignisse von diesem EKS-Cluster. Dies kann sich auf Ihre Nutzungsstatistiken auswirken. 2. Um zu verhindern, dass Tags, außer durch vertrauen swürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *`ec2: CreateTags`* durch `eks:TagResource` . • Ersetzen Sie *`ec2: DeleteTags`* durch. `eks:UntagResource`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen Sie *access-project* durch `GuardDutyManaged` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Unabhängig davon, wie Sie den Security Agent verwalten (über GuardDuty oder manuell), müssen Sie den bereitgestellten Security Agent aus diesem EKS-Cluster entfernen, um den Empfang von Runtime-Ereignissen von diesem Cluster zu beenden. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie unter Auswirkungen der Deaktivierung und Bereinigung von Ressourcen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster mithilfe von Einschließen-Tags überwachen	1. Aktivieren Sie auf der Seite Konten nach der Aktivierung von Runtime Monitoring nicht Runtime Monitoring — Automated Agent configuration. 2. Fügen Sie dem EKS-Cluster ein Tag hinzu, das zu dem ausgewählten Konto gehört, das Sie überwachen möchten. Das Schlüssel-Wert-Paar des Tags muss `GuardDutyManaged -true` sein. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. GuardDuty verwaltet die Verteilung und Aktualisierung des Security Agents für die ausgewählten EKS-Cluster, die Sie überwachen möchten. 3. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Verwalten Sie den Security Agent manuell GuardDuty	1. Stellen Sie sicher, dass Sie im Abschnitt Automatisierte Agentenkonfiguration nicht die Option Aktivieren auswählen. Lassen Sie Runtime Monitoring aktiviert. 2. Wählen Sie Speichern. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster.

Automatische Aktivierung der automatischen Agentenkonfiguration für neue Mitglieder

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Alle EKS-Cluster überwachen)	1. Wählen Sie auf der Seite Runtime Monitoring die Option Bearbeiten, um die bestehende Konfiguration zu aktualisieren. 2. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Automatisch für neue Mitgliedskonten aktivieren aus. 3. Wählen Sie Speichern.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft. Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent nicht auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource`. • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged`. • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen:

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte

```
"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
```

3. Öffnen Sie die Konsole unter https://console.aws.amazon.com/guardduty/ GuardDuty .
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.

> **Note**
>
> Fügen Sie Ihren EKS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto installiert.

5. Wählen Sie auf der Registerkarte Konfiguration im Bereich GuardDuty Agentenverwaltung die Option Automatisch für neue Mitgliedskonten aktivieren aus.

   Für die EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden, GuardDuty wird die Bereitstellung und Aktualisierung des GuardDuty Security Agents verwaltet.
6. Wählen Sie Speichern.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent auf diesem Cluster installiert wurde 1. Unabhängig davon, ob Sie den GuardDuty Security Agent über GuardDuty oder manuell verwalten, fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und dem Wert as hinzu`false`. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. Wenn Sie den Automated Agent für diesen EKS-Cluster aktiviert hatten, GuardDuty wird der Security Agent für diesen Cluster nach diesem Schritt nicht aktualisiert. Der Security Agent bleibt jedoch weiterhin installiert und empfängt GuardDuty weiterhin die Runtime-Ereignisse von diesem EKS-Cluster. Dies kann sich auf Ihre Nutzungsstatistiken auswirken. Um die Laufzeit-Ereignisse von diesem Cluster nicht mehr zu empfangen, müssen Sie den bereitgestellten Sicherheitsagent aus diesem EKS-Cluster entfernen. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie unter Auswirkungen der Deaktivierung und Bereinigung von Ressourcen 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben:

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDuty Managed` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Wenn Sie den GuardDuty Security Agent für diesen EKS-Cluster manuell verwaltet haben, finden Sie weitere Informationen unter. Auswirkungen der Deaktivierung und Bereinigung von Ressourcen

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster mithilfe von Einschließen-Tags überwachen	Unabhängig davon, wie Sie Runtime Monitoring aktiviert haben, helfen Ihnen die folgenden Schritte bei der Überwachung ausgewählter EKS-Cluster auf die neuen Mitgliedskonten in Ihrer Organisation. 1. Stellen Sie sicher, dass im Abschnitt Automatisierte Agentenkonfiguration die Option Automatisch für neue Mitgliedskonten aktivieren deaktiviert ist. Behalten Sie die Runtime Monitoring-Konfiguration bei, die Sie im vorherigen Schritt konfiguriert haben. 2. Wählen Sie Speichern. 3. Fügen Sie Ihrem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `true` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. GuardDuty verwaltet die Verteilung und Aktualisierung des Security Agents für die ausgewählten EKS-Cluster, die Sie überwachen möchten. 4. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *`ec2: CreateTags`* durch `eks:TagResource` . • Ersetzen Sie *`ec2: DeleteTags`* durch. `eks:UntagResource`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen Sie *access-project* durch `GuardDuty Managed` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Verwalten Sie den Security Agent manuell GuardDuty	Unabhängig davon, wie Sie Runtime Monitoring aktiviert haben, können Sie den Security Agent für Ihre EKS-Cluster manuell verwalten. 1. Stellen Sie sicher, dass das Kontrollkästchen Automatisch für neue Mitgliedskonten aktivieren im Abschnitt Automatische Agentenkonfiguration deaktiviert ist. Behalten Sie die Runtime Monitoring-Konfiguration bei, die Sie im vorherigen Schritt konfiguriert haben. 2. Wählen Sie Speichern. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster.

Selektives Konfigurieren des automatisierten Agenten für aktive Mitgliedskonten

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Alle EKS-Cluster überwachen)	1. Wählen Sie auf der Seite Konten die Konten aus, für die Sie die automatische Agentenkonfiguration aktivieren möchten. Sie können mehr als ein Konto zur gleichen Zeit auswählen. Stellen Sie sicher, dass für die Konten, die Sie in diesem Schritt auswählen, EKS-Laufzeit-Überwachung bereits aktiviert ist. 2. Wählen Sie unter Schutzpläne bearbeiten die entsprechende Option aus, um Runtime Monitoring — Automatisierte Agentenkonfiguration zu aktivieren. 3. Wählen Sie Bestätigen aus.
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft. Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent nicht auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben:

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDuty Managed` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Öffnen Sie die Konsole unter https://console.aws.amazon.com/guardduty/ GuardDuty . **Note** Fügen Sie Ihren EKS-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto bereitgestellt. 4. Wählen Sie auf der Kontenseite das Konto aus, für das Sie Agent automatisch verwalten aktivieren möchten. Sie können mehr als ein Konto zur gleichen Zeit auswählen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	5. Wählen Sie unter Schutzpläne bearbeiten die entsprechende Option aus, um die automatische Agentenkonfiguration mit Runtime Monitoring für das ausgewählte Konto zu aktivieren. Verwaltet bei EKS-Clustern, die nicht von der Überwachung ausgeschlossen wurden, GuardDuty die Bereitstellung und Aktualisierung des Security Agents. GuardDuty 6. Wählen Sie Speichern. Um einen EKS-Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `false` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. Wenn Sie zuvor die automatische Agentenkonfiguration für diesen EKS-Cluster aktiviert hatten, GuardDuty wird der Security Agent für diesen Cluster nach diesem Schritt nicht aktualisi ert. Der Security Agent bleibt jedoch weiterhin installiert und empfängt GuardDuty weiterhin die Runtime-Ereignisse von diesem EKS-Cluster. Dies kann sich auf Ihre Nutzungsstatistiken auswirken. Um die Laufzeit-Ereignisse von diesem Cluster nicht mehr zu empfangen, müssen Sie den bereitgestellten Sicherheitsagent aus diesem EKS-Cluster entfernen. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie unter Auswirkungen der Deaktivierung und Bereinigung von Ressourcen

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDuty Managed` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Wenn Sie den GuardDuty Security Agent für diesen EKS-Cluster manuell verwaltet haben, müssen Sie ihn entfernen. Weitere Informationen finden Sie unter Auswirkungen der Deaktivierung und Bereinigung von Ressourcen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster mithilfe von Einschließen-Tags überwachen	Unabhängig davon, wie Sie Runtime Monitoring aktiviert haben, helfen Ihnen die folgenden Schritte bei der Überwachung ausgewählter EKS-Cluster, die zu den ausgewählten Konten gehören: 1. Stellen Sie sicher, dass Sie die automatische Agentenkonfiguration mit Runtime Monitoring nicht für die ausgewählten Konten aktivieren, die über die EKS-Cluster verfügen, die Sie überwachen möchten. 2. Fügen Sie Ihrem EKS-Cluster ein Tag mit dem Schlüssel als `GuardDutyManaged` und seinem Wert als `true` hinzu. Weitere Informationen zum Markieren Ihres Amazon-EKS-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im Amazon-EKS-Benutzerhandbuch. Nach dem Hinzufügen des Tags GuardDuty werden die Verteilung und Aktualisierung des Security Agents für die ausgewählten EKS-Cluster, die Sie überwachen möchten, verwaltet. 3. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *`ec2: CreateTags`* durch `eks:TagResource` . • Ersetzen Sie *`ec2: DeleteTags`* durch. `eks:UntagResource` • Ersetzen Sie *`access-project`* durch `GuardDutyManaged` .

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Verwalten Sie den Security Agent manuell GuardDuty	1. Behalten Sie für die Runtime Monitoring-Konfiguration dieselbe wie im vorherigen Schritt bei. Stellen Sie sicher, dass Sie für keines der ausgewählten Konten die automatische Agentenkonfiguration von Runtime Monitoring aktivieren. 2. Wählen Sie Bestätigen aus. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster.

Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster

In diesem Abschnitt wird beschrieben, wie Sie Ihren Amazon EKS-Add-On-Agenten (GuardDuty Agenten) verwalten können, nachdem Sie Runtime Monitoring aktiviert haben. Um Runtime Monitoring verwenden zu können, müssen Sie Runtime Monitoring aktivieren und das Amazon EKS-Add-on konfigurieren`aws-guardduty-agent`. Wenn Sie nur einen dieser beiden Schritte ausführen, können Sie potenzielle Bedrohungen nicht GuardDuty erkennen oder Ergebnisse generieren.

Voraussetzungen für die Installation des GuardDuty Security Agents

In diesem Abschnitt werden die Voraussetzungen für die manuelle Installation des GuardDuty Security Agents für Ihre EKS-Cluster beschrieben. Bevor Sie fortfahren, stellen Sie sicher, dass

Sie Runtime Monitoring bereits für Ihre Konten konfiguriert haben. Der GuardDuty Security Agent (EKS-Add-on) funktioniert nicht, wenn Sie Runtime Monitoring nicht konfigurieren. Weitere Informationen finden Sie unter GuardDuty Runtime Monitoring aktivieren. Nachdem Sie diese Schritte abgeschlossen haben, sehen Sie Der Security Agent wird bereitgestellt GuardDuty .

Wählen Sie Ihre bevorzugte Zugriffsmethode, um einen Amazon-VPC-Endpunkt zu erstellen.

Console

VPC-Endpunkt erstellen

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsmenü unter Virtual Private Cloud die Option Endpunkte.
3. Klicken Sie auf Endpunkt erstellen.
4. Wählen Sie auf der Seite Endpunkt erstellen für Servicekategorie die Option Andere Endpunkt-Services.
5. Geben Sie unter Servicename **`com.amazonaws.`*`us-east-1`*`.guardduty-data`** ein.

   Stellen Sie sicher, dass Sie *`us-east-1`* durch die richtige Region ersetzen. Dies muss dieselbe Region sein wie der EKS-Cluster, der zu Ihrer AWS-Konto ID gehört.
6. Wählen Sie Service verifizieren.
7. Nachdem der Servicename erfolgreich verifiziert wurde, wählen Sie die VPC aus, in der sich Ihr Cluster befindet. Fügen Sie die folgende Richtlinie hinzu, um die Nutzung von VPC-Endpunkten auf das angegebene Konto zu beschränken. Unter Angabe der unter dieser Richtlinie angegebenen Organisations-`Condition` können Sie die folgende Richtlinie aktualisieren, um den Zugriff auf Ihren Endpunkt einzuschränken. Informationen zur Bereitstellung von VPC-Endpunktunterstützung für bestimmte Konto-IDs in Ihrer Organisation finden Sie unter Organization condition to restrict access to your endpoint.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
```

```
    "Condition": {
     "StringNotEquals": {
      "aws:PrincipalAccount": "111122223333"
     }
    },
    "Action": "*",
    "Resource": "*",
    "Effect": "Deny",
    "Principal": "*"
   }
  ]
}
```

Die `aws:PrincipalAccount`-Konto-ID muss mit dem Konto übereinstimmen, das die VPC und den VPC-Endpunkt enthält. Die folgende Liste zeigt, wie Sie den VPC-Endpunkt mit anderen AWS-Konto -IDs teilen können:

Organisationsbedingung , um den Zugriff auf Ihren Endpunkt einzuschränken

- Um mehrere Konten für den Zugriff auf den VPC-Endpunkt anzugeben, ersetzen Sie `"aws:PrincipalAccount": "111122223333"` durch Folgendes:

```
"aws:PrincipalAccount": [
          "666666666666",
          "555555555555"
    ]
```

- Um allen Mitgliedern einer Organisation den Zugriff auf den VPC-Endpunkt zu ermöglichen, ersetzen Sie `"aws:PrincipalAccount": "111122223333"` durch Folgendes:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- Um den Zugriff auf eine Ressource auf eine Organisations-ID zu beschränken, fügen Sie Ihre `ResourceOrgID` zur Richtlinie hinzu.

  Weitere Informationen finden Sie unter ResourceOrgID.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. Wählen Sie unter Zusätzliche Einstellungen die Option DNS-Name aktivieren.
9. Wählen Sie unter Subnetze die Subnetze aus, in denen sich Ihr Cluster befindet.

10. Wählen Sie unter Sicherheitsgruppen eine Sicherheitsgruppe aus, für die der eingehende Port 443 von Ihrer VPC (oder Ihrem EKS-Cluster) aktiviert ist. Wenn Sie noch keine Sicherheitsgruppe haben, für die der eingehende Port 443 aktiviert ist, Erstellen Sie eine Sicherheitsgruppe.

    Wenn bei der Einschränkung der eingehenden Berechtigungen für Ihre VPC (oder Ihren Cluster) ein Problem auftritt, stellen Sie die Unterstützung für den eingehenden Port 443 von einer beliebigen IP-Adresse (`0.0.0.0/0`) bereit.

API/CLI

- Aufrufen CreateVpcEndpoint.
- Verwenden Sie die folgenden Werte für die Parameter:
  - Geben Sie unter Servicename **`com.amazonaws.`*`us-east-1`*`.guardduty-data`** ein.

    Stellen Sie sicher, dass Sie *`us-east-1`* durch die richtige Region ersetzen. Dies muss dieselbe Region sein wie der EKS-Cluster, der zu Ihrer AWS-Konto ID gehört.
  - Aktivieren Sie für DNSOptions die private DNS-Option, indem Sie sie auf `true` setzen.
- AWS Command Line Interface Näheres dazu finden Sie unter create-vpc-endpoint.

Konfigurieren Sie die Parameter des GuardDuty Security Agents (Add-On) für Amazon EKS

Sie können spezifische Parameter Ihres GuardDuty Security Agents für Amazon EKS konfigurieren. Diese Unterstützung ist für GuardDuty Security Agent Version 1.5.0 und höher verfügbar. Informationen zu den neuesten Add-On-Versionen finden Sie unterGuardDuty Sicherheitsagent für Amazon EKS-Cluster.

Warum sollte ich das Security Agent Konfigurationsschema aktualisieren

Das Konfigurationsschema für den GuardDuty Security Agent ist für alle Container in Ihren Amazon EKS-Clustern dasselbe. Wenn die Standardwerte nicht mit den zugehörigen Workloads und der Instance-Größe übereinstimmen, sollten Sie die Konfiguration der CPU-Einstellungen, Speichereinstellungen und `dnsPolicy` Einstellungen in Betracht ziehen. `PriorityClass` Unabhängig davon, wie Sie den GuardDuty Agenten für Ihre Amazon EKS-Cluster verwalten, können Sie die bestehende Konfiguration dieser Parameter konfigurieren oder aktualisieren.

Automatisiertes Verhalten der Agentenkonfiguration mit konfigurierten Parametern

Wenn er den Security Agent (EKS-Add-on) in Ihrem Namen GuardDuty verwaltet, aktualisiert er das Add-on bei Bedarf. GuardDuty setzt den Wert der konfigurierbaren Parameter auf einen Standardwert. Sie können die Parameter jedoch immer noch auf einen gewünschten Wert aktualisieren. Wenn dies zu einem Konflikt führt, ist die Standardoption für ResolveConflicts. None

Konfigurierbare Parameter und Werte

Informationen zu den Schritten zur Konfiguration der Zusatzparameter finden Sie unter:

- Der Security Agent wird bereitgestellt GuardDuty oder
- Manuelles Aktualisieren des Security Agents

Die folgenden Tabellen enthalten die Bereiche und Werte, die Sie verwenden können, um das Amazon EKS-Add-on manuell bereitzustellen oder die vorhandenen Add-On-Einstellungen zu aktualisieren.

CPU-Einstellungen

Parameter	Standardwert	Konfigurierbarer Bereich
Anforderungen	200m	Zwischen 200 m und 10000 m, beide inklusive
Einschränkungen	1000m	

Speicher-Einstellungen

Parameter	Standardwert	Konfigurierbarer Bereich
Anforderungen	256 Mi	Zwischen 256Mi und 20000Mi, beide inklusive
Einschränkungen	1024 Mi	

`PriorityClass`-Einstellungen

Wenn Sie GuardDuty ein Amazon EKS-Add-on für Sie erstellen, `PriorityClass` ist das zugewieseneaws-guardduty-agent.priorityclass. Das bedeutet, dass aufgrund

der Priorität des Agenten-Pods keine Maßnahmen ergriffen werden. Sie können diesen Zusatzparameter konfigurieren, indem Sie eine der folgenden `PriorityClass` Optionen wählen:

Konfigurierbar **`PriorityClass`**	**`preemptionPolicy`** Wert	**`preemptionPolicy`** Beschreibung	Pod-Wert
`aws-guardduty-agent.priorityclass`	`Never`	Keine Aktion	1000000
`aws-guardduty-agent.priorityclass-high`	`PreemptLowerPriority`	Durch die Zuweisung dieses Werts wird verhindert, dass ein Pod ausgeführt wird, dessen Prioritätswert unter dem Pod-Wert des Agenten liegt.	100000000
`system-cluster-critical` [1]	`PreemptLowerPriority`		2000000000
`system-node-critical` [1]	`PreemptLowerPriority`		2000001000

[1] Kubernetes bietet diese beiden `PriorityClass` Optionen — und. `system-cluster-critical` `system-node-critical` Weitere Informationen finden Sie PriorityClassin der Kubernetes-Dokumentation.

`dnsPolicy`-Einstellungen

Wählen Sie eine der folgenden DNS-Richtlinienoptionen, die Kubernetes unterstützt. Wird als Standardwert verwendet, wenn keine Konfiguration angegeben `ClusterFirst` ist.

- `ClusterFirst`
- `ClusterFirstWithHostNet`
- `Default`

Informationen zu diesen Richtlinien finden Sie in der Kubernetes-Dokumentation unter DNS-Richtlinie von Pod.

Der Security Agent wird bereitgestellt GuardDuty

In diesem Abschnitt wird beschrieben, wie Sie den GuardDuty Security Agent zum ersten Mal für bestimmte EKS-Cluster einsetzen können. Bevor Sie mit diesem Abschnitt fortfahren, stellen Sie sicher, dass Sie die Voraussetzungen bereits eingerichtet und Runtime Monitoring für Ihre Konten aktiviert haben. Der GuardDuty Security Agent (EKS-Add-on) funktioniert nicht, wenn Sie Runtime Monitoring nicht aktivieren.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty Security Agent zum ersten Mal zu installieren.

Console

1. Öffnen Sie die Amazon-EKS-Konsole unter https://console.aws.amazon.com/eks/home#/clusters.
2. Wählen Sie Ihren Clusternamen aus.
3. Wählen Sie die Registerkarte Add-ons.
4. Wählen Sie Weitere Add-Ons erhalten.
5. Wählen Sie auf der Seite „Add-Ons auswählen“ Amazon GuardDuty Runtime Monitoring aus.
6. Verwenden Sie auf der Seite Ausgewählte Add-On-Einstellungen konfigurieren die Standardeinstellungen. Wenn der Status Ihres EKS-Add-ons Aktivierung erfordert lautet, wählen Sie Aktivieren aus GuardDuty. Diese Aktion öffnet die GuardDuty Konsole, in der Sie Runtime Monitoring für Ihre Konten konfigurieren können.
7. Nachdem Sie Runtime Monitoring für Ihre Konten konfiguriert haben, kehren Sie zur Amazon EKS-Konsole zurück. Der Status Ihres EKS-Add-Ons sollte sich auf Bereit zur Installation geändert haben.
8. (Optional) Bereitstellung des Konfigurationsschemas für das EKS-Add-On

   Wenn Sie für die Add-On-Version Version v1.5.0 und höher wählen, unterstützt Runtime Monitoring die Konfiguration bestimmter GuardDuty Agentenparameter. Hinweise zu Parameterbereichen finden Sie unterKonfigurieren Sie die EKS-Zusatzparameter.

   a. Erweitern Sie Optionale Konfigurationseinstellungen, um die konfigurierbaren Parameter sowie deren erwarteten Wert und Format anzuzeigen.

   b. Stellen Sie die Parameter ein. Die Werte müssen in dem angegebenen Bereich liegenKonfigurieren Sie die EKS-Zusatzparameter.

c. Wählen Sie Änderungen speichern, um das Add-on auf der Grundlage der erweiterten Konfiguration zu erstellen.

d. Bei der Methode zur Konfliktlösung wird die von Ihnen gewählte Option verwendet, um einen Konflikt zu lösen, wenn Sie den Wert eines Parameters auf einen anderen Wert als den Standardwert aktualisieren. Weitere Informationen zu den aufgelisteten Optionen finden Sie unter ResolveConflicts in der Amazon EKS-API-Referenz.

9. Wählen Sie Weiter aus.
10. Überprüfen Sie auf der Seite Überprüfen und erstellen alle Details und wählen Sie dann Erstellen.
11. Gehen Sie zurück zu den Cluster-Details und wählen Sie die Registerkarte Ressourcen.
12. Sie können die neuen Pods mit dem Präfix anzeigen. aws-guardduty-agent

API/CLI

Sie können den Amazon-EKS-Add-On-Agent (`aws-guardduty-agent`) konfigurieren, indem Sie eine der folgenden Optionen verwenden:

- Starte CreateAddonfür dein Konto.
-

> **Note**
>
> Wenn Sie für das Add-on `version` Version 1.5.0 und höher wählen, unterstützt Runtime Monitoring die Konfiguration bestimmter GuardDuty Agentenparameter. Weitere Informationen finden Sie unter Konfigurieren Sie die EKS-Zusatzparameter.

Verwenden Sie die folgenden Werte für die Parameter:

- Geben Sie unter `addonName` den Wert `aws-guardduty-agent` ein.

Sie können das folgende AWS CLI Beispiel verwenden, wenn Sie konfigurierbare Werte verwenden, die für die Addon-Versionen v1.5.0 und höher unterstützt werden. Achten Sie darauf, die rot markierten Platzhalterwerte und die `Example.json` mit den konfigurierten Werten verknüpften Werte zu ersetzen.

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

Example example.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

- Weitere Informationen zu unterstützten `addonVersion` finden Sie unter Kubernetes-Versionen, die vom Security Agent unterstützt werden GuardDuty .

- Alternativ können Sie verwenden. AWS CLI Weitere Informationen finden Sie unter create-addon.

Manuelles Aktualisieren des Security Agents

Wenn Sie den GuardDuty Security Agent manuell verwalten, sind Sie dafür verantwortlich, ihn für Ihr Konto zu aktualisieren. Um über neue Agent-Versionen informiert zu werden, können Sie einen RSS-Feed abonnierenGuardDuty Versionsverlauf des Agenten.

Sie können den Security Agent auf die neueste Version aktualisieren, um von der zusätzlichen Unterstützung und den Verbesserungen zu profitieren. Wenn der Standardsupport für Ihre aktuelle Agentenversion ausläuft, müssen Sie Ihre aktuelle Agentenversion aktualisieren, um Runtime Monitoring (oder EKS Runtime Monitoring) weiterhin verwenden zu können. Informationen zu Release-Versionen finden Sie unterGuardDuty Sicherheitsagent für Amazon EKS-Cluster.

Voraussetzung

Bevor Sie die Security Agent-Version aktualisieren, stellen Sie sicher, dass die Agent-Version, die Sie jetzt verwenden möchten, mit Ihrer Kubernetes-Version kompatibel ist. Weitere Informationen finden Sie unter Kubernetes-Versionen, die vom Security Agent unterstützt werden GuardDuty .

Console

1. Öffnen Sie die Amazon-EKS-Konsole unter https://console.aws.amazon.com/eks/home#/clusters.
2. Wählen Sie Ihren Clusternamen aus.
3. Wählen Sie Add-Ons.
4. Wählen Sie unter Add-Ons die Option GuardDutyRuntime Monitoring aus.
5. Wählen Sie Bearbeiten, um die Agentendetails zu aktualisieren.
6. Aktualisieren Sie auf der Seite GuardDuty Runtime Monitoring konfigurieren die Details.
7. (Optional) Aktualisierung der Konfigurationsparameter des Add-ons

   Wenn Ihre EKS-Add-On-Version 1.5.0 oder höher ist, können Sie auch die Add-On-Konfigurationseinstellungen aktualisieren.

   a. Erweitern Sie Optionale Konfigurationseinstellungen, um das Konfigurationsschema anzuzeigen.
   b. Aktualisieren Sie die Parameterwerte basierend auf dem angegebenen Bereich unterKonfigurieren Sie die EKS-Zusatzparameter.
   c. Wählen Sie Änderungen speichern, um das Update zu starten.
   d. Bei der Methode zur Konfliktlösung wird die von Ihnen gewählte Option verwendet, um einen Konflikt zu lösen, wenn Sie den Wert eines Parameters auf einen Wert aktualisieren, der nicht dem Standard entspricht. Weitere Informationen zu den aufgelisteten Optionen finden Sie unter ResolveConflicts in der Amazon EKS-API-Referenz.

API/CLI

Informationen zum Update des GuardDuty Security Agents für Ihre Amazon EKS-Cluster finden Sie unter Ein Add-on aktualisieren.

> **Note**
>
> Wenn Sie für das Add-on `version` Version 1.5.0 und höher wählen, unterstützt Runtime Monitoring die Konfiguration bestimmter GuardDuty Agentenparameter. Hinweise zu Parameterbereichen finden Sie unterKonfigurieren Sie die EKS-Zusatzparameter.

Sie können das folgende AWS CLI Beispiel verwenden, wenn Sie konfigurierbare Werte verwenden, die für die Addon-Versionen v1.5.0 und höher unterstützt werden. Achten Sie darauf, die rot markierten Platzhalterwerte und die `Example.json` mit den konfigurierten Werten verknüpften Werte zu ersetzen.

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

Example example.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

Wenn Ihre Amazon EKS-Add-On-Version 1.5.0 oder höher ist und Sie das Add-On-Schema konfiguriert haben, können Sie überprüfen, ob die Werte für Ihren Cluster korrekt angezeigt werden. Weitere Informationen finden Sie unter Aktualisierungen des Konfigurationsschemas werden überprüft.

Aktualisierungen des Konfigurationsschemas werden überprüft

Nachdem Sie die Parameter konfiguriert haben, führen Sie die folgenden Schritte aus, um zu überprüfen, ob das Konfigurationsschema aktualisiert wurde:

1. Öffnen Sie die Amazon-EKS-Konsole unter https://console.aws.amazon.com/eks/home#/clusters.
2. Klicken Sie im Navigationsbereich auf Cluster.

3. Wählen Sie auf der Seite Cluster den Clusternamen aus, für den Sie die Updates überprüfen möchten.
4. Wählen Sie die Registerkarte Resources (Ressourcen) aus.
5. Wählen Sie im Bereich Ressourcentypen unter Workloads die Option DaemonSets.
6. Select aws-guardduty-agent.
7. Wählen Sie auf der aws-guardduty-agentSeite die Option Rohansicht aus, um die unformatierte JSON-Antwort anzuzeigen. Stellen Sie sicher, dass die konfigurierbaren Parameter den von Ihnen angegebenen Wert anzeigen.

Wechseln Sie nach der Überprüfung zur GuardDuty Konsole. Wählen Sie das entsprechende aus AWS-Region und sehen Sie sich den Deckungsstatus für Ihre Amazon EKS-Cluster an. Weitere Informationen finden Sie unter Abdeckung für Amazon EKS-Cluster.

Konfiguration von EKS Runtime Monitoring (nur API)

Bevor Sie die EKS-Laufzeit-Überwachung in Ihrem Konto konfigurieren, stellen Sie sicher, dass Sie eine der verifizierten Plattformen verwenden, die die derzeit verwendete Kubernetes-Version unterstützt. Weitere Informationen finden Sie unter Validierung der architektonischen Anforderungen.

EKS-Laufzeit-Überwachung für ein eigenständiges Konto konfigurieren

Informationen zu den Konten, die AWS Organizations zugeordnet sind, finden Sie unterKonfiguration der EKS-Laufzeit-Überwachung für Umgebungen mit mehreren Konten.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die EKS-Laufzeit-Überwachung für Ihr Konto zu aktivieren.

API/CLI

Auf der Grundlage von Methoden zur Verwaltung des GuardDuty Security Agents können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Security Agent verwalten über GuardDuty (Alle EKS-Cluster überwachen)	1. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster in Ihrem Konto. 2. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -false`. Weitere Informationen zum

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** Fügen Sie Ihrem EKS-Cluster immer das Ausschluss-Tag hinzu, bevor Sie das `STATUS`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	von EKS_RUNTIME_MONITORING auf setzen. ENABLED Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto installiert. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den features-Objektnamen als EKS_RUNTIME_MONITORING und den Status als ENABLED übergeben. Stellen Sie den Status für EKS_ADDON_MANAGEMENT als ENABLED ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die detectorId für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert sowohl EKS_RUNTIME_MONITORING als auch EKS_ADDON_MANAGEMENT : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "Addition` Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den features-Objektnamen als EKS_RUNTIME_MONITORING und den Status als ENABLED übergeben. Stellen Sie den Status für EKS_ADDON_MANAGEMENT als ENABLED ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die detectorId für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert sowohl EKS_RUNTIME_MONITORING als auch EKS_ADDON_MANAGEMENT : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "Addition`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	alConfiguration" : [{"Name" : "EKS_ADDO N_MANAGEMENT", "Status" : " *ENABLED*"}]]'

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster überwachen (mithilfe des Einschließen-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -true`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource`. • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged`. • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die mit dem `true` -Paar `GuardDutyManaged` -gekennzeichnet wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Sicherheitsagent manuell verwalten	1. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster.

Konfiguration der EKS-Laufzeit-Überwachung für Umgebungen mit mehreren Konten

In Umgebungen mit mehreren Konten kann nur das delegierte GuardDuty Administratorkonto EKS Runtime Monitoring für die Mitgliedskonten aktivieren oder deaktivieren und die GuardDuty Agentenverwaltung für die EKS-Cluster verwalten, die zu den Mitgliedskonten in ihrer Organisation gehören. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten.

Konfiguration von EKS Runtime Monitoring für das delegierte Administratorkonto GuardDuty

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Runtime Monitoring zu aktivieren und den GuardDuty Security Agent für die EKS-Cluster zu verwalten, die zum delegierten GuardDuty Administratorkonto gehören.

API/CLI

Auf der Grundlage von Methoden zur Verwaltung des GuardDuty Security Agents können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Security Agent verwalten über GuardDuty (Alle EKS-Cluster überwachen)	Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster in Ihrem Konto.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -false`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource`. • Ersetzen Sie *ec2: DeleteTags* durch `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged`. • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. **Note** Fügen Sie Ihrem EKS-Cluster immer das Ausschluss-Tag hinzu, bevor Sie das `STATUS` von `EKS_RUNTIME_MONITORING` auf `ENABLED` setzen. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto installiert. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` :

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	`aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster überwachen (mithilfe des Einschließen-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -true`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource`. • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged`. • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die mit dem `true` -Paar `GuardDutyManaged` -gekennzeichnet wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Sicherheitsagent manuell verwalten	1. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'` 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster.

Automatische Aktivierung der EKS-Laufzeit-Überwachung für alle Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die EKS-Laufzeit-Überwachung für alle Mitgliedskonten zu aktivieren. Dazu gehören das delegierte GuardDuty Administratorkonto, bestehende Mitgliedskonten und die neuen Konten, die der Organisation beitreten. Wählen Sie Ihren bevorzugten Ansatz zur Verwaltung des GuardDuty Security Agents für die EKS-Cluster, die zu diesen Mitgliedskonten gehören.

API/CLI

Auf der Grundlage von Methoden zur Verwaltung des GuardDuty Security Agents können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Security Agent verwalten über GuardDuty (Alle EKS-Cluster überwachen)	Um die EKS-Laufzeit-Überwachung selektiv für Ihre Mitglieds konten zu aktivieren, führen Sie den API-Vorgang updateMem berDetectors mit Ihrer eigenen *Detektor-ID* aus. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster in Ihrem Konto. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon .com/guardduty/ -Konsole. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITO RING` als auch `EKS_ADDON_MANAGEMENT` :

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0    --account-
ids 111122223333  --features '[{"Name" : "EKS_RUNT
IME_MONITORING", "Status" : "  ENABLED", "Addition
alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT",
 "Status" : "ENABLED"}] ]'
```

> **Note**
>
> Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -false`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. **Note** Fügen Sie Ihrem EKS-Cluster immer das Ausschluss-Tag hinzu, bevor Sie das `STATUS` von `EKS_RUNTIME_MONITORING` auf `ENABLED` setzen. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto installiert. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden. Alternativ können Sie den AWS CLI Befehl verwenden , indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	ids *111122223333* --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " *ENABLED*", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " *ENABLED*"}]]'

> **Note**
>
> Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster überwachen (mithilfe des Einschließen-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -true`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die mit dem `true` -Paar `GuardDutyManaged` - gekennzeichnet wurden. Alternativ können Sie den AWS CLI Befehl verwenden , indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstell ungen“ in der https://console.aws.amazon.com/guardduty/ - Konsole. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITO RING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Sicherheitsagent manuell verwalten	1. Führen Sie die updateDetector-API aus, indem Sie Ihre eigene regionale Detektor-ID verwenden und den `features`-Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als `ENABLED` übergeben. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden , indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstell ungen“ in der https://console.aws.amazon.com/guardduty/ - Konsole. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITO RING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster.

Konfiguration der EKS-Laufzeit-Überwachung für alle vorhandenen aktiven Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Runtime Monitoring zu aktivieren und den GuardDuty Security Agent für bestehende aktive Mitgliedskonten in Ihrer Organisation zu verwalten.

API/CLI

Auf der Grundlage von Methoden zur Verwaltung des GuardDuty Security Agents können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Security Agent verwalten über GuardDuty (Alle EKS-Cluster überwachen)	Um die EKS-Laufzeit-Überwachung selektiv für Ihre Mitglieds konten zu aktivieren, führen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen *Detektor-ID* aus. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster in Ihrem Konto. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	> **Note** > Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind. Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -false`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. **Note** Fügen Sie Ihrem EKS-Cluster immer das Ausschluss-Tag hinzu, bevor Sie das `STATUS` von `EKS_RUNTIME_MONITORING` auf `ENABLED` setzen. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto installiert. Um die EKS-Laufzeit-Überwachung selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen *`Detektor-ID`* aus. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "Addition``

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEM ENT", "Status" : " *ENABLED*"}]]' **Note** Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind. Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster überwachen (mithilfe des Einschließen-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -true`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource` . • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged` . • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. Um die EKS-Laufzeit-Überwachung selektiv für Ihre Mitglieds konten zu aktivieren, führen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen *Detektor-ID* aus. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die mit dem `true` -Paar `GuardDutyManaged` - gekennzeichnet wurden. Alternativ können Sie den AWS CLI Befehl verwenden , indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstell ungen“ in der https://console.aws.amazon.com/guardduty/ - Konsole. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITO RING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.
Den Sicherheitsagent manuell verwalten	1. Um die EKS-Laufzeit-Überwachung selektiv für Ihre Mitglieds konten zu aktivieren, führen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen *`Detektor-ID`* aus. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden , indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstell ungen“ in der https://console.aws.amazon.com/guardduty/ - Konsole. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITO RING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster.

EKS-Laufzeit-Überwachung für neue Mitglieder automatisch aktivieren

Das delegierte GuardDuty Administratorkonto kann EKS Runtime Monitoring automatisch aktivieren und einen Ansatz für die Verwaltung des GuardDuty Security Agents für neue Konten wählen, die Ihrer Organisation beitreten.

API/CLI

Auf der Grundlage von Methoden zur Verwaltung des GuardDuty Security Agents können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
Den Security Agent verwalten über GuardDuty (Alle EKS-Cluster überwachen)	Um die EKS-Laufzeit-Überwachung selektiv für Ihre neuen Konten zu aktivieren, rufen Sie den API-Vorgang UpdateOrganizationConfiguration mit Ihrer eigenen *Detektor-ID* auf. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster in Ihrem Konto. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Im folgenden Beispiel werden beide Optionen `EKS_RUNTIME_MONITORING` und `EKS_ADDON_MANAGEMENT` für ein einzelnes Konto aktiviert. Sie können auch eine

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -false`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource`. • Ersetzen Sie *ec2: DeleteTags* durch `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged`. • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	3. **Note** Fügen Sie Ihrem EKS-Cluster immer das Ausschluss-Tag hinzu, bevor Sie das `STATUS` von `EKS_RUNTIME_MONITORING` auf setzen. `ENABLED` Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto installiert. Um die EKS-Laufzeit-Überwachung selektiv für Ihre neuen Konten zu aktivieren, rufen Sie den API-Vorgang UpdateOrganizationConfiguration mit Ihrer eigenen *`Detektor-ID`* auf. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Im folgenden Beispiel werden beide Optionen `EKS_RUNTIME_MONITORING` und `EKS_ADDON_MANAGEMENT` für ein einzelnes Konto aktiviert.

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	Sie können auch eine Liste von Konto-IDs übergeben , die durch ein Leerzeichen getrennt sind. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
Ausgewählte EKS-Cluster überwachen (mithilfe des Einschließen-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -true`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource`. • Ersetzen Sie *ec2: DeleteTags* durch. `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged`. • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	3. Um die EKS-Laufzeit-Überwachung selektiv für Ihre neuen Konten zu aktivieren, rufen Sie den API-Vorgang UpdateOrganizationConfiguration mit Ihrer eigenen *Detektor-ID* auf. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die mit dem `true` -Paar `GuardDutyManaged` -gekennzeichnet wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` für ein einzelnes Konto. Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING",`

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	`"AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
Den Sicherheitsagent manuell verwalten	1. Um die EKS-Laufzeit-Überwachung selektiv für Ihre neuen Konten zu aktivieren, rufen Sie den API-Vorgang UpdateOrganizationConfiguration mit Ihrer eigenen *Detektor-ID* auf. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` für ein einzelnes Konto. Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'`

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt. 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster.

EKS-Laufzeit-Überwachung für einzelne aktive Mitgliedskonten aktivieren

API/CLI

Auf der Grundlage von Methoden zur Verwaltung des GuardDuty Security Agents können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Security Agent verwalten über GuardDuty (Alle EKS-Cluster überwachen)	Um die EKS-Laufzeit-Überwachung selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen *`Detektor-ID`* aus. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster in Ihrem Konto.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'` **Note** Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind. Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Alle EKS-Cluster überwachen, jedoch einige davon ausschließen (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -false`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource`. • Ersetzen Sie *ec2: DeleteTags* durch `eks:UntagResource` • Ersetzen Sie *access-project* durch `GuardDutyManaged`. • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. **Note** Fügen Sie Ihrem EKS-Cluster immer das Ausschluss-Tag hinzu, bevor Sie das `STATUS` von `EKS_RUNTIME_MONITORING` auf `ENABLED` setzen. Andernfalls wird der GuardDuty Security Agent auf allen EKS-Clustern in Ihrem Konto installiert. Um die EKS-Laufzeit-Überwachung selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen *`Detektor-ID`* aus. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die nicht von der Überwachung ausgeschlossen wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` :

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	`aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'` **Note** Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind. Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Ausgewählte EKS-Cluster überwachen (mithilfe des Einschließen-Tags)	1. Fügen Sie dem EKS-Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -true`. Weitere Informationen zum Hinzufügen eines Tags finden Sie unter Arbeiten mit Tags mithilfe der CLI, API oder eksctl im Amazon-EKS-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen Sie *ec2: CreateTags* durch `eks:TagResource`. • Ersetzen Sie *ec2: DeleteTags* durch `eks:UntagResource`. • Ersetzen Sie *access-project* durch `GuardDutyManaged`. • Ersetzen Sie *123456789012* durch die AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. Um die EKS-Laufzeit-Überwachung selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen *Detektor-ID* aus. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle Amazon EKS-Cluster, die mit dem `true` -Paar `GuardDutyManaged` -gekennzeichnet wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	> **Note** > Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind. Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Sicherheitsagent manuell verwalten	1. Um die EKS-Laufzeit-Überwachung selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen *Detektor-ID* aus. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Die `detectorId` für Ihr Konto und Ihre aktuelle Region geltenden Einstellungen finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für den Amazon EKS-Cluster.

Migration von EKS Runtime Monitoring zu Runtime Monitoring

Mit der Einführung von GuardDuty Runtime Monitoring wurde der Geltungsbereich der Bedrohungserkennung auf Amazon ECS-Container und Amazon EC2 EC2-Instances ausgeweitet. EKS Runtime Monitoring wurde nun in Runtime Monitoring konsolidiert. Sie können Runtime Monitoring aktivieren und einzelne GuardDuty Security Agents für jeden Ressourcentyp (Amazon EC2 EC2-Instance, Amazon ECS-Cluster und Amazon EKS-Cluster) verwalten, für den Sie das Laufzeitverhalten überwachen möchten.

Für EKS Runtime Monitoring gibt es keine separate GuardDuty Konsolenerfahrung. Um EKS Runtime Monitoring weiterhin verwenden zu können, müssen Sie es mithilfe von APIs oder dem konfigurieren AWS Command Line Interface.

Um von EKS Runtime Monitoring zu Runtime Monitoring zu migrieren

1. Die GuardDuty Konsole unterstützt EKS Runtime Monitoring als Teil von Runtime Monitoring.

   Sie können damit beginnen, Runtime Monitoring Überprüfen Sie den Konfigurationsstatus von EKS Runtime Monitoring von Ihrer Organisation und Ihren Konten aus zu verwenden.

   Stellen Sie sicher, dass Sie EKS Runtime Monitoring nicht deaktivieren, bevor Sie Runtime Monitoring aktivieren. Wenn Sie EKS Runtime Monitoring deaktivieren, wird auch die Amazon EKS Add-On-Verwaltung deaktiviert. Fahren Sie mit den folgenden Schritten in der angegebenen Reihenfolge fort.
2. Stellen Sie sicher, dass Sie alle erfüllenVoraussetzungen für die Aktivierung von Runtime Monitoring.
3. Aktivieren Sie die Laufzeit-Überwachung, indem Sie die gleichen Einstellungen der Organisationskonfiguration für die Laufzeit-überwachung replizieren wie für die EKS-Laufzeit-Überwachung. Weitere Informationen finden Sie unter Laufzeitüberwachung aktivieren.
   - Wenn Sie ein eigenständiges Konto haben, müssen Sie Runtime Monitoring aktivieren.

     Wenn Ihr GuardDuty Security Agent bereits installiert ist, werden die entsprechenden Einstellungen automatisch repliziert und Sie müssen die Einstellungen nicht erneut konfigurieren.
   - Wenn Sie eine Organisation mit Einstellungen für die automatische Aktivierung haben, stellen Sie sicher, dass Sie dieselben Einstellungen für die automatische Aktivierung für Runtime Monitoring replizieren.

- Wenn Sie ein Unternehmen haben, dessen Einstellungen für bestehende aktive Mitgliedskonten einzeln konfiguriert sind, stellen Sie sicher, dass Sie Runtime Monitoring aktivieren und den GuardDuty Security Agent für diese Mitglieder individuell konfigurieren.

4. Nachdem Sie sichergestellt haben, dass die Einstellungen für Runtime Monitoring und GuardDuty Security Agent korrekt sind, deaktivieren Sie EKS Runtime Monitoring, indem Sie entweder die API oder den AWS CLI Befehl verwenden.
5. (Optional) Wenn Sie alle mit dem GuardDuty Security Agent verknüpften Ressourcen säubern möchten, finden Sie weitere Informationen unterAuswirkungen der Deaktivierung und Bereinigung von Ressourcen.

Wenn Sie EKS Runtime Monitoring weiterhin verwenden möchten, ohne Runtime Monitoring zu aktivieren, finden Sie weitere Informationen unterKonfiguration von EKS Runtime Monitoring (nur API).

Überprüfen Sie den Konfigurationsstatus von EKS Runtime Monitoring

Verwenden Sie die folgenden APIs oder AWS CLI Befehle, um den bestehenden Konfigurationsstatus von EKS Runtime Monitoring zu überprüfen.

Um den bestehenden EKS Runtime Monitoring-Konfigurationsstatus in Ihrem Konto zu überprüfen

- Führen Sie den Befehl aus GetDetector, um den Konfigurationsstatus Ihres eigenen Kontos zu überprüfen.
- Alternativ können Sie den folgenden Befehl ausführen, indem Sie Folgendes verwenden AWS CLI:

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1
```

Achten Sie darauf, die Melder-ID Ihrer Region AWS-Konto und der aktuellen Region zu ersetzen. Die `detectorId` für Ihr Konto und Ihre aktuelle Region passende finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

Um den bestehenden EKS Runtime Monitoring-Konfigurationsstatus für Ihre Organisation zu überprüfen (nur als delegiertes GuardDuty Administratorkonto)

- Führen Sie das DescribeOrganizationConfigurationProgramm aus, um den Konfigurationsstatus Ihrer Organisation zu überprüfen.

Alternativ können Sie den folgenden Befehl ausführen mit AWS CLI:

```
aws guardduty describe-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
```

Achten Sie darauf, die Melder-ID durch die Melder-ID Ihres delegierten GuardDuty Administratorkontos und die Region durch Ihre aktuelle Region zu ersetzen. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

Deaktivieren von EKS Runtime Monitoring nach der Migration zu Runtime Monitoring

Nachdem Sie sichergestellt haben, dass die vorhandenen Einstellungen für Ihr Konto oder Ihre Organisation in Runtime Monitoring repliziert wurden, können Sie EKS Runtime Monitoring deaktivieren.

Um EKS Runtime Monitoring zu deaktivieren

- Um EKS Runtime Monitoring in Ihrem eigenen Konto zu deaktivieren

  Führen Sie die UpdateDetectorAPI mit Ihrer eigenen regionalen *Detektor-ID* aus.

  Alternativ können Sie den folgenden AWS CLI Befehl verwenden. *Ersetzen Sie 12abc34d567e8fa901bc2d34e56789f0 durch Ihre eigene regionale Detektor-ID.*

  ```
  aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "DISABLED"}]'
  ```

- Um EKS Runtime Monitoring für Mitgliedskonten in Ihrer Organisation zu deaktivieren

  Führen Sie die UpdateMemberDetectorsAPI mit der regionalen *Detektor-ID* des delegierten GuardDuty Administratorkontos der Organisation aus.

  Alternativ können Sie den folgenden Befehl verwenden. AWS CLI *Ersetzen Sie 12abc34d567e8fa901bc2d34e56789f0 durch die regionale Detektor-ID des delegierten GuardDuty Administratorkontos der Organisation und*

111122223333 durch die ID des Mitgliedskontos, für das Sie diese Funktion deaktivieren möchten. AWS-Konto

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",
 "Status" : "DISABLED"}]'
```

- Um die Einstellungen für die automatische Aktivierung von EKS Runtime Monitoring für Ihre Organisation zu aktualisieren

  Führen Sie den folgenden Schritt nur aus, wenn Sie die Einstellungen für die automatische Aktivierung von EKS Runtime Monitoring entweder auf neue (`NEW`) oder alle (`ALL`) Mitgliedskonten in der Organisation konfiguriert haben. Wenn Sie es bereits als konfiguriert haben`NONE`, können Sie diesen Schritt überspringen.

  > **Note**
  >
  > Wenn Sie die Konfiguration für die automatische Aktivierung von EKS Runtime `NONE` Monitoring auf einstellen, wird EKS Runtime Monitoring nicht automatisch für ein vorhandenes Mitgliedskonto aktiviert oder wenn ein neues Mitgliedskonto Ihrer Organisation beitritt.

  Führen Sie die UpdateOrganizationConfigurationAPI mit der regionalen *Detektor-ID* des delegierten GuardDuty Administratorkontos der Organisation aus.

  Alternativ können Sie den folgenden Befehl verwenden. AWS CLI *Ersetzen Sie 12abc34d567e8fa901bc2d34e56789f0 durch die regionale Detektor-ID des delegierten Administratorkontos der Organisation.* GuardDuty Ersetzen Sie *EXISTING_VALUE* durch Ihre aktuelle Konfiguration für die automatische Aktivierung. GuardDuty

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
   --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
  ```

Bewertung der Laufzeitabdeckung Ihrer Ressourcen

Nachdem Sie Runtime Monitoring aktiviert haben und der GuardDuty Security Agent auf Ihrer Ressource installiert wurde, GuardDuty liefert er Deckungsstatistiken für den entsprechenden Ressourcentyp und den individuellen Schutzstatus für die Ressourcen, die zu Ihrem Konto gehören. Der Deckungsstatus wird bestimmt, indem Sie sicherstellen, dass Sie Runtime Monitoring aktiviert haben, Ihr Amazon VPC-Endpunkt erstellt wurde und der GuardDuty Security Agent für die entsprechende Ressource bereitgestellt wurde. Der Coverage-Status „Fehlerfrei“ gibt an, dass, wenn es ein Laufzeitereignis im Zusammenhang mit Ihrer Ressource gibt, GuardDuty das besagte Laufzeitereignis über den Amazon VPC-Endpunkt empfangen und das Verhalten überwachen kann. Wenn bei der Konfiguration von Runtime Monitoring, der Erstellung eines Amazon VPC-Endpunkts oder der Bereitstellung des GuardDuty Security Agents ein Problem aufgetreten ist, wird der Deckungsstatus als Ungesund angezeigt. Wenn der Deckungsstatus fehlerhaft ist, kann GuardDuty das Laufzeitverhalten der entsprechenden Ressource nicht empfangen oder überwacht werden, und es können auch keine Runtime Monitoring-Ergebnisse generiert werden.

Die folgenden Themen helfen Ihnen dabei, Deckungsstatistiken zu überprüfen, EventBridge Benachrichtigungen zu konfigurieren und Probleme mit der Abdeckung für einen bestimmten Ressourcentyp zu beheben.

Inhalt

Deckung für Amazon EC2 EC2-Instance

Für eine Amazon EC2 EC2-Ressource wird die Laufzeitabdeckung auf Instance-Ebene bewertet. Ihre Amazon EC2 EC2-Instances können unter anderem mehrere Arten von Anwendungen und Workloads in Ihrer AWS Umgebung ausführen. Diese Funktion unterstützt auch von Amazon ECS verwaltete Amazon EC2 EC2-Instances. Wenn Sie Amazon ECS-Cluster auf einer Amazon EC2 EC2-Instance ausführen, werden die Deckungsprobleme auf Instance-Ebene unter Amazon EC2 EC2-Laufzeitabdeckung angezeigt.

Themen

- Überprüfen der Abdeckungsstatistiken
- Benachrichtigungen über Änderungen des Abdeckungsstatus konfigurieren
- Fehlerbehebung bei Abdeckungsproblemen

Überprüfen der Abdeckungsstatistiken

Die Deckungsstatistik für die Amazon EC2 EC2-Instances, die Ihren eigenen Konten oder Ihren Mitgliedskonten zugeordnet sind, ist der Prozentsatz der fehlerfreien EC2-Instances an allen EC2-Instances in den ausgewählten. AWS-Region Die folgende Gleichung stellt dies wie folgt dar:

(Fehlerfreie Instanzen/Alle Instances) *100

Wenn Sie den GuardDuty Security Agent auch für Ihre Amazon ECS-Cluster bereitgestellt haben, wird jedes Problem mit der Abdeckung auf Instance-Ebene im Zusammenhang mit Amazon ECS-Clustern, die auf einer Amazon EC2 EC2-Instance ausgeführt werden, als ein Problem mit der Laufzeit der Amazon EC2 EC2-Instance angezeigt.

Wählen Sie eine der Zugriffsmethoden, um die Abdeckungsstatistiken für Ihre Konten einzusehen.

Console

- Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
- Wählen Sie im Navigationsbereich Runtime Monitoring aus.
- Wählen Sie die Registerkarte Runtime Coverage aus.
- Auf der Registerkarte EC2-Instance-Laufzeitabdeckung können Sie die Deckungsstatistiken einsehen, die nach dem Deckungsstatus jeder Amazon EC2 EC2-Instance aggregiert sind, die in der Tabelle mit der Instance-Liste verfügbar sind.
  - Sie können die Tabelle mit der Instance-Liste nach den folgenden Spalten filtern:
    - Konto-ID
    - Agentenverwaltungs-Typ
    - Version des Agenten
    - Abdeckungsstatus
    - Instanz-ID
    - Cluster-ARN

- Wenn eine Ihrer EC2-Instances den Coverage-Status als Unhealthy hat, enthält die Spalte Issue zusätzliche Informationen über den Grund für den Status Unhealthy.

API/CLI

- Führen Sie die ListCoverageAPI mit Ihrer eigenen gültigen Melder-ID, Ihrer aktuellen Region und Ihrem Service-Endpunkt aus. Mit dieser API können Sie die Instanzliste filtern und sortieren.
  - Sie können das Beispiel `filter-criteria` ändern mit einer der folgenden Optionen für `CriterionKey`:
    - `ACCOUNT_ID`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `AGENT_VERSION`
    - `MANAGEMENT_TYPE`
    - `INSTANCE_ID`
    - `CLUSTER_ARN`
  - Wenn EC2 **`filter-criteria`** enthalten `RESOURCE_TYPE` ist, unterstützt Runtime Monitoring nicht die Verwendung von ISSUE als. `AttributeName` Wenn Sie es verwenden, führt die API-Antwort zu`InvalidInputException`.

    Sie können das Beispiel `AttributeName` in `sort-criteria` ändern mit einer der folgenden Optionen:
    - `ACCOUNT_ID`
    - `COVERAGE_STATUS`
    - `INSTANCE_ID`
    - `UPDATED_AT`
  - Sie können *`max-results`* ändern (bis zu 50).
  - Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ - Konsole.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
```

```
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Führen Sie die GetCoverageStatisticsAPI aus, um aggregierte Statistiken zur Abdeckung abzurufen, die `statisticsType` auf dem basieren.
  - Sie können das Beispiel `statisticsType` zu einer der folgenden Optionen ändern:
    - `COUNT_BY_COVERAGE_STATUS` – Stellt Abdeckungsstatistiken für EKS-Cluster dar, aggregiert nach Abdeckungs-Status.
    - `COUNT_BY_RESOURCE_TYPE`— Statistiken zur Abdeckung, aggregiert auf der Grundlage des AWS Ressourcentyps in der Liste.
    - Sie können das Beispiel `filter-criteria` im Befehl ändern. Sie können die folgenden Optionen für `CriterionKey` verwenden:
      - `ACCOUNT_ID`
      - `RESOURCE_TYPE`
      - `COVERAGE_STATUS`
      - `AGENT_VERSION`
      - `MANAGEMENT_TYPE`
      - `INSTANCE_ID`
      - `CLUSTER_ARN`
  - Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Wenn der Deckungsstatus Ihrer EC2-Instance Unhealthy lautet, finden Sie weitere Informationen unter. Fehlerbehebung bei Abdeckungsproblemen

Benachrichtigungen über Änderungen des Abdeckungsstatus konfigurieren

Der Deckungsstatus Ihrer Amazon EC2 EC2-Instance wird möglicherweise als Ungesund angezeigt. Um zu wissen, wann sich der Deckungsstatus ändert, empfehlen wir Ihnen, den Deckungsstatus regelmäßig zu überwachen und Fehler zu beheben, falls der Status auf Ungesund umgestellt wird. Alternativ können Sie eine EventBridge Amazon-Regel erstellen, um eine Benachrichtigung zu erhalten, wenn sich der Versicherungsstatus von „Ungesund“ in „Fehlerfrei“ oder anderweitig ändert. GuardDuty Veröffentlicht dies standardmäßig im EventBridge Bus für Ihr Konto.

Beispiel für ein Benachrichtigungsschema

In einer EventBridge Regel können Sie die vordefinierten Beispielereignisse und Ereignismuster verwenden, um Benachrichtigungen über den Versicherungsstatus zu erhalten. Weitere Informationen zum Erstellen einer EventBridge Regel finden Sie unter Regel erstellen im EventBridge Amazon-Benutzerhandbuch.

Darüber hinaus können Sie mithilfe des folgenden Beispiel-Benachrichtigungsschemas ein benutzerdefiniertes Ereignismuster erstellen. Achten Sie darauf, die Werte für Ihr Konto zu ersetzen. Um benachrichtigt zu werden, wenn sich der Deckungsstatus Ihrer Amazon EC2 EC2-Instance von `Healthy` zu ändert`Unhealthy`, `detail-type` sollte *`GuardDuty Runtime Protection Unhealthy lauten`*. Um benachrichtigt zu werden, wenn sich der Deckungsstatus von `Unhealthy` auf ändert`Healthy`, ersetzen Sie den Wert von `detail-type` durch *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS-Konto ID",
  "time": "event timestamp (string)",
  "region": "AWS-Region",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EC2",
```

```
        "ec2InstanceDetails": {
          "instanceId":"",
          "instanceType":"",
          "clusterArn": "",
          "agentDetails": {
            "version":""
          },
          "managementType":""
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Fehlerbehebung bei Abdeckungsproblemen

Wenn der Deckungsstatus Ihrer Amazon EC2 EC2-Instance Unhealthy lautet, können Sie den Grund in der Spalte Problem einsehen.

Wenn Ihre EC2-Instance einem EKS-Cluster zugeordnet ist und der Security Agent für EKS entweder manuell oder über eine automatische Agentenkonfiguration installiert wurde, finden Sie Informationen zur Behebung des Deckungsproblems unter. Abdeckung für Amazon EKS-Cluster

In der folgenden Tabelle sind die Problemtypen und die entsprechenden Schritte zur Fehlerbehebung aufgeführt.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Keine Berichterstattung durch Agenten	Ich warte auf die SSM-Benachrichtigung	Stellen Sie sicher, dass die Amazon EC2 EC2-Instance bereits SSM-verwaltet wird. Der Empfang der SSM-Benachrichtigung kann einige Minuten dauern.
	(Absichtlich leer)	Wenn Sie den GuardDuty Security Agent manuell verwalten, stellen Sie sicher, dass Sie die Schritte unter befolgt habenManuelles Verwalten des Security Agents für Amazon EC2 EC2-Instance.
		Wenn Sie die automatische Agentenkonfiguration aktiviert haben:

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
		• Ihre EC2-Instance wird SSM-verwaltet. • Sehen Sie sich regelmäßig den Status Ihres Security Agents an. Weitere Informationen finden Sie unter Der Installationsstatus des GuardDuty Security Agents wird überprüft.
		Wenn Ihr Unternehmen über eine Service Control Policy (SCP) verfügt, stellen Sie sicher, dass die `guardduty:SendSecurityTelemetry` Genehmigung nicht verweigert wird. Weitere Informationen finden Sie unter Überprüfung der Service-Control-Richtlinie Ihrer Organisation.
	Die Verbindung des Agenten wurde unterbrochen	• Sehen Sie sich den Status Ihres Security Agents an. Weitere Informationen finden Sie unter Der Installationsstatus des GuardDuty Security Agents wird überprüft. • Sehen Sie sich die Security Agent-Protokolle an, um die mögliche Ursache zu ermitteln. Die Protokolle enthalten detaillierte Fehler, anhand derer Sie das Problem selbst beheben können. Die Protokolldateien sind verfügbar unter `/var/log/amzn-guardduty-agent/` . `Tunsudo journalctl -u amazon-guardduty-agent .`

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Die Erstellung der SSM-Zuordnung ist fehlgeschlagen	GuardDuty In Ihrem Konto ist bereits eine SSM-Verknüpfung vorhanden	1. Löschen Sie die bestehende Verknüpfung manuell. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Löschen von Verknüpfungen. 2. Nachdem Sie die Zuordnung gelöscht haben, deaktivieren Sie die GuardDuty automatische Agentenkonfiguration für Amazon EC2 und aktivieren Sie sie anschließend erneut.
	Ihr Konto hat zu viele SSM-Verknüpfungen	Wählen Sie eine der folgenden beiden Optionen: • Löschen Sie alle ungenutzten SSM-Verknüpfungen. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Löschen von Verknüpfungen. • Prüfen Sie, ob Ihr Konto für eine Erhöhung des Kontingents in Frage kommt. Weitere Informationen finden Sie unter Systems Manager Manager-Dienstkontingente in der Allgemeine AWS-Referenz.
Die Aktualisierung der SSM-Zuordnung ist fehlgeschlagen	GuardDuty Die SSM-Verknüpfung ist in Ihrem Konto nicht vorhanden	GuardDuty Die SSM-Verbindung ist in Ihrem Konto nicht vorhanden. Deaktivieren Sie Runtime Monitoring und aktivieren Sie es anschließend erneut.
Das Löschen der SSM-Zuordnung ist fehlgeschlagen	GuardDuty Die SSM-Verknüpfung ist in Ihrem Konto nicht vorhanden	Die SSM-Verbindung ist in Ihrem Konto nicht vorhanden. Wenn die SSM-Verknüpfung absichtlich gelöscht wurde, sind keine Maßnahmen erforderlich.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Die Ausführung der SSM-Insta nzzuweisung ist fehlgeschlagen	Architektonische Anforderungen oder andere Vorausset zungen sind nicht erfüllt.	Informationen zu verifizierten Betriebssystemverteilungen finden Sie unterVoraussetzungen für die Unterstützung von Amazon EC2 EC2-Instances. Wenn dieses Problem weiterhin auftritt, helfen Ihnen die folgenden Schritte dabei, das Problem zu identifizieren und möglicherweise zu lösen: 1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/. 2. Wählen Sie im Navigationsbereich unter Node Management die Option State Manager aus. 3. Filtern Sie nach der Eigenschaft Dokumentname und geben Sie ein AmazonGuardDuty-ConfigureRu ntimeMonitoringSsmPlugin. 4. Wählen Sie die entsprechende Zuordnungs-ID aus und sehen Sie sich den zugehörigen Ausführun gsverlauf an. 5. Sehen Sie sich anhand des Ausführungsverlaufs die Fehler an, identifizieren Sie die potenzielle Ursache und versuchen Sie, sie zu beheben.
VPC-Endpu nkterstellung ist fehlgeschlagen	VPC-Endpu nkterstel lung wird für gemeinsam genutzte VPC *vpcId* nicht unterstützt	Runtime Monitoring unterstützt die Verwendung einer gemeinsam genutzten VPC innerhalb einer Organisation. Weitere Informationen finden Sie unter Verwenden einer gemeinsam genutzten VPC mit automatisierten Sicherhei tsagenten.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
	Nur bei Verwendung einer gemeinsam genutzten VPC mit automatisierter Agentenkonfiguration Die Besitzerkonto-ID *111122223333* für gemeinsam genutzte *VPC-VPCid* hat weder Runtime Monitoring noch automatische Agentenkonfiguration oder beides aktiviert	Das gemeinsame VPC-Besitzerkonto muss Runtime Monitoring und automatische Agentenkonfiguration für mindestens einen Ressourcentyp (Amazon EKS oder Amazon ECS (AWS Fargate)) aktivieren. Weitere Informationen finden Sie unter Spezifische Voraussetzungen für Runtime Monitoring GuardDuty.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
	Um privates DNS zu aktiviere n, müssen sowohl das enableDns Support - als auch das enableDns Hostnames -VPC-Attr ibute für vpcId auf true gesetzt sein (Service: Ec2, Status Code:400, Request ID: a1b2c3d4- 5678-90ab -cdef-EXA MPLE11111).	Sie müssen jedoch sicherstellen, dass die folgenden VPC-Attribute auf `true` festgelegt sind: `enableDns Support` und `enableDnsHostnames` . Weitere Informationen finden Sie unter DNS-Attribute in Ihrer VPC. Wenn Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/ verwenden, um die Amazon VPC zu erstellen, stellen Sie sicher, dass Sie sowohl DNS-Hostnamen aktivieren als auch DNS-Auflö sung aktivieren auswählen. Weitere Informationen finden Sie unter VPC-Konfigurationsoptionen.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Fehler beim Löschen eines gemeinsamen VPC-Endpunkts	*Das Löschen eines gemeinsamen VPC-Endpunkts ist für die Konto-ID 111122223333 , die gemeinsame VPC-VPC-ID , die Besitzerkonto-ID 555555555 nicht zulässig.*	Mögliche Schritte: • Die Deaktivierung des Runtime Monitoring-Status des gemeinsam genutzten VPC-Teilnehmerkontos hat keine Auswirkungen auf die gemeinsame VPC-Endpunktrichtlinie und die Sicherheitsgruppe, die im Besitzerkonto vorhanden ist. Um den gemeinsamen VPC-Endpunkt und die Sicherheitsgruppe zu löschen, müssen Sie Runtime Monitoring oder den Status der automatisierten Agentenkonfiguration im gemeinsam genutzten VPC-Besitzerkonto deaktivieren. • Das gemeinsame VPC-Teilnehmerkonto kann den gemeinsamen VPC-Endpunkt und die Sicherheitsgruppe, die im gemeinsamen VPC-Besitzerkonto gehostet werden, nicht löschen.
Der Agent meldet sich nicht	(Absichtlich leer)	Der Support für diesen Problemtyp hat das Ende des Supports erreicht. Wenn dieses Problem weiterhin auftritt und dies noch nicht geschehen ist, aktivieren Sie den GuardDuty automatisierten Agenten für Amazon EC2. Wenn das Problem weiterhin besteht, sollten Sie in Erwägung ziehen, Runtime Monitoring für einige Minuten zu deaktivieren und es dann erneut zu aktivieren.

Abdeckung für Amazon ECS-Cluster

Die Laufzeitabdeckung für Amazon ECS-Cluster umfasst die Aufgaben, die auf AWS Fargate (Fargate) Amazon ECS-Container-Instances ausgeführt werden [1].

Für einen Amazon ECS-Cluster, der auf Fargate läuft, wird die Laufzeitabdeckung auf Aufgabenebene bewertet. Die Laufzeitabdeckung des ECS-Clusters umfasst die Fargate-Aufgaben,

die gestartet wurden, nachdem Sie Runtime Monitoring und automatisierte Agentenkonfiguration für Fargate aktiviert haben (nur ECS). Standardmäßig ist eine Fargate-Aufgabe unveränderlich. GuardDuty wird nicht in der Lage sein, den Security Agent zur Überwachung von Containern bei bereits laufenden Aufgaben zu installieren. Um eine solche Fargate-Aufgabe einzubeziehen, müssen Sie die Aufgabe beenden und erneut starten. Stellen Sie sicher, dass Sie überprüfen, ob der zugehörige Dienst unterstützt wird.

Derzeit unterstützt Runtime Monitoring die von AWS CodePipeline gestarteten Aufgaben nicht.

Informationen zum Amazon ECS-Container finden Sie unter Kapazitätserstellung.

Inhalt

Überprüfen der Abdeckungsstatistiken

Die Deckungsstatistik für die Amazon ECS-Ressourcen, die mit Ihrem eigenen Konto oder Ihren Mitgliedskonten verknüpft sind, ist der Prozentsatz der fehlerfreien Amazon ECS-Cluster im Vergleich zu allen Amazon ECS-Clustern in den ausgewählten AWS-Region. Dies beinhaltet die Abdeckung für Amazon ECS-Cluster, die sowohl mit Fargate- als auch mit Amazon EC2 EC2-Instances verknüpft sind. Die folgende Gleichung stellt dies wie folgt dar:

(Fehlerfreie Cluster/Alle Cluster)*100

Überlegungen

- Die Deckungsstatistiken für den ECS-Cluster beinhalten den Abdeckungsstatus der Fargate-Aufgaben oder ECS-Container-Instances, die diesem ECS-Cluster zugeordnet sind. Der Deckungsstatus der Fargate-Aufgaben umfasst Aufgaben, die sich entweder im Status Running befinden oder deren Ausführung vor Kurzem abgeschlossen wurde.
- Auf der Registerkarte Runtime Coverage von ECS-Clustern gibt das Feld Abgedeckte Container-Instances den Abdeckungsstatus der Container-Instances an, die Ihrem Amazon ECS-Cluster zugeordnet sind.

  Wenn Ihr Amazon ECS-Cluster nur Fargate-Aufgaben enthält, wird die Anzahl als 0/0 angezeigt.

- Wenn Ihr Amazon ECS-Cluster mit einer Amazon EC2 EC2-Instance verknüpft ist, die keinen Sicherheitsagenten hat, hat der Amazon ECS-Cluster auch den Status Unhealthy Coverage.

  Informationen zur Identifizierung und Behebung des Deckungsproblems für die zugehörige Amazon EC2 EC2-Instance finden Sie unter Fehlerbehebung bei Abdeckungsproblemen Amazon EC2 EC2-Instances.

Wählen Sie eine der Zugriffsmethoden, um die Abdeckungsstatistiken für Ihre Konten einzusehen.

Console

- Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
- Wählen Sie im Navigationsbereich Runtime Monitoring aus.
- Wählen Sie die Registerkarte Runtime Coverage aus.
- Auf der Registerkarte ECS-Cluster-Laufzeitabdeckung können Sie die Deckungsstatistiken einsehen, die nach dem Abdeckungsstatus jedes Amazon ECS-Clusters aggregiert sind, der in der Cluster-Listentabelle verfügbar ist.
  - Sie können die Cluster-Listentabelle nach den folgenden Spalten filtern:
    - Konto-ID
    - Clustername
    - Agentenverwaltungs-Typ
    - Abdeckungsstatus
- Wenn einer Ihrer Amazon ECS-Cluster den Deckungsstatus Ungesund hat, enthält die Spalte Problem zusätzliche Informationen über den Grund für den Status Ungesund.

  Wenn Ihre Amazon ECS-Cluster mit einer Amazon EC2 EC2-Instance verknüpft sind, navigieren Sie zur Registerkarte EC2-Instance-Laufzeitabdeckung und filtern Sie nach dem Feld Clustername, um das zugehörige Problem anzuzeigen.

API/CLI

- Führen Sie die ListCoverageAPI mit Ihrer eigenen gültigen Detektor-ID, Ihrer aktuellen Region und Ihrem Service-Endpunkt aus. Mit dieser API können Sie die Instanzliste filtern und sortieren.

- Sie können das Beispiel `filter-criteria` ändern mit einer der folgenden Optionen für `CriterionKey`:
  - `ACCOUNT_ID`
  - `ECS_CLUSTER_NAME`
  - `COVERAGE_STATUS`
  - `MANAGEMENT_TYPE`
- Sie können das Beispiel `AttributeName` in `sort-criteria` ändern mit einer der folgenden Optionen:
  - `ACCOUNT_ID`
  - `COVERAGE_STATUS`
  - `ISSUE`
  - `ECS_CLUSTER_NAME`
  - `UPDATED_AT`

    Das Feld wird nur aktualisiert, wenn entweder eine neue Aufgabe im zugehörigen Amazon ECS-Cluster erstellt wird oder wenn sich der entsprechende Deckungsstatus ändert.
- Sie können *`max-results`* ändern (bis zu 50).
- Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "ECS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Führen Sie die GetCoverageStatisticsAPI aus, um aggregierte Statistiken zur Abdeckung abzurufen, die `statisticsType` auf dem basieren.
  - Sie können das Beispiel `statisticsType` zu einer der folgenden Optionen ändern:
    - `COUNT_BY_COVERAGE_STATUS`— Stellt Deckungsstatistiken für ECS-Cluster dar, die nach dem Abdeckungsstatus aggregiert sind.
    - `COUNT_BY_RESOURCE_TYPE`— Statistiken zur Abdeckung, aggregiert auf der Grundlage des AWS Ressourcentyps in der Liste.

  - Sie können das Beispiel `filter-criteria` im Befehl ändern. Sie können die folgenden Optionen für `CriterionKey` verwenden:
    - `ACCOUNT_ID`
    - `ECS_CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `MANAGEMENT_TYPE`
    - `INSTANCE_ID`
- Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ - Konsole.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Weitere Informationen zu Problemen mit der Netzabdeckung finden Sie unterFehlerbehebung bei Abdeckungsproblemen.

Benachrichtigungen über Änderungen des Abdeckungsstatus konfigurieren

Der Abdeckungsstatus Ihres Amazon ECS-Clusters wird möglicherweise als Ungesund angezeigt. Um zu wissen, wann sich der Deckungsstatus ändert, empfehlen wir Ihnen, den Deckungsstatus regelmäßig zu überwachen und Fehler zu beheben, falls der Status auf Ungesund umgestellt wird. Alternativ können Sie eine EventBridge Amazon-Regel erstellen, um eine Benachrichtigung zu erhalten, wenn sich der Versicherungsstatus von „Ungesund“ in „Fehlerfrei“ oder anderweitig ändert. GuardDuty Veröffentlicht dies standardmäßig im EventBridge Bus für Ihr Konto.

Beispiel für ein Benachrichtigungsschema

In einer EventBridge Regel können Sie die vordefinierten Beispielereignisse und Ereignismuster verwenden, um Benachrichtigungen über den Versicherungsstatus zu erhalten. Weitere Informationen zum Erstellen einer EventBridge Regel finden Sie unter Regel erstellen im EventBridge Amazon-Benutzerhandbuch.

Darüber hinaus können Sie mithilfe des folgenden Beispiel-Benachrichtigungsschemas ein benutzerdefiniertes Ereignismuster erstellen. Achten Sie darauf, die Werte für Ihr Konto zu ersetzen.

Um benachrichtigt zu werden, wenn sich der Abdeckungsstatus Ihres Amazon ECS-Clusters von `Healthy` zu ändert`Unhealthy`, `detail-type` sollte *`GuardDuty Runtime Protection Unhealthy lauten`*. Um benachrichtigt zu werden, wenn sich der Deckungsstatus von `Unhealthy` zu ändert`Healthy`, ersetzen Sie den Wert von `detail-type` durch *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS-Konto ID",
  "time": "event timestamp (string)",
  "region": "AWS-Region",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "ECS",
        "ecsClusterDetails": {
          "clusterName":"",
          "fargateDetails":{
            "issues":[],
            "managementType":""
          },
          "containerInstanceDetails":{
            "coveredContainerInstances":int,
            "compatibleContainerInstances":int
          }
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Fehlerbehebung bei Abdeckungsproblemen

Wenn der Abdeckungsstatus Ihres Amazon ECS-Clusters fehlerhaft ist, können Sie den Grund in der Spalte Problem einsehen.

Die folgende Tabelle enthält die empfohlenen Schritte zur Fehlerbehebung bei Fargate-Problemen (nur Amazon ECS). Informationen zu Problemen mit der Abdeckung von Amazon EC2 EC2-Instances finden Sie unter Fehlerbehebung bei Abdeckungsproblemen Für Amazon EC2 EC2-Instances.

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbeh ebung
Der Agent meldet sich nicht	Der Agent meldet sich nicht für Aufgaben in `TaskDefinition - '`*`TASK_DEFINITION`*`'`	Stellen Sie sicher, dass Ihre VPC-Endpu nktkonfiguration korrekt ist. Wenn Ihre Organisation über eine Service Control Policy (SCP) verfügt, stellen Sie sicher, dass die Genehmigu ng nicht verweigert wird. `guardduty :SendSecurityTelemetry` Weitere Informationen finden Sie unter Überprüfung der Service-Kontroll-R ichtlinie Ihres Unternehmens.
	`VPC_ISSUE` `; for task in TaskDefin ition - '` *`TASK_DEFI NITION`* `'`	Einzelheiten zum VPC-Problem finden Sie in den zusätzlichen Informationen.
Der Agent wurde beendet	ExitCode: `EXIT_CODE` für Aufgaben in `TaskDefinition - '`*`TASK_DEFINITION`*`'`	Die Problemdetails finden Sie in den zusätzlichen Informationen.
	Grund: *`GRUND`* für Aufgaben in `TaskDefin ition - '` *`TASK_DEFI NITION`* `'`	

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbeh ebung
	ExitCode: `EXIT_CODE` mit Grund: '*`EXIT_CODE`* ' für Aufgaben in `TaskDefinition` - '*`TASK_DEFINITION`* '	

	Der Agent wurde beendet: `GrundCannotPul lContainerError` : Das Abrufen des Image-Manifests wurde erneut versucht...	Die Aufgabenausführungsrolle muss über die folgenden Amazon Elastic Container Registry (Amazon ECR) - Berechtigungen verfügen:
		`...`
		`"ecr:GetAuthorizat ionToken",`
		`"ecr:BatchCheckLay erAvailability",`
		`"ecr:GetDownloadUr lForLayer",`
		`"ecr:BatchGetImage",`
		`...`
		Weitere Informationen finden Sie unter Geben Sie ECR-Berechtigungen und Subnetzdetails an.
		Nachdem Sie die Amazon ECR-Berec htigungen hinzugefügt haben, müssen Sie die Aufgabe neu starten.
		Wenn das Problem weiterhin besteht, finden Sie weitere Informationen unter. Mein AWS Step Functions Workflow schlägt unerwartet fehl

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbeh ebung
Andere oder nicht bereitgestellter Agent	Unbekanntes Problem, für Aufgaben in `TaskDefinition - '`*`TASK_DEFINITION`*` '`	Ermitteln Sie anhand der folgenden Fragen die Ursache des Problems: • Wurde die Aufgabe gestartet, bevor Sie Runtime Monitoring aktiviert haben? In Amazon ECS sind die Aufgaben unveränderlich. Um das Laufzeitv erhalten einer laufenden Fargate-Aufgabe zu beurteilen, stellen Sie sicher, dass Runtime Monitoring bereits aktiviert ist, und starten Sie dann die Aufgabe neu, GuardDuty um den Container-Sidecar hinzuzufügen. • Wurde die Aufgabe von einem Dienst gestartet, der nicht unterstützt wird? Derzeit unterstützt Runtime Monitorin g die von gestarteten Aufgaben nicht. AWS CodePipeline • Ist diese Aufgabe Teil einer Dienstber eitstellung, die gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben? Falls ja, können Sie den Dienst entweder neu starten oder den Dienst mit aktualisieren, `forceNewD eployment` indem Sie die Schritte unter Dienst aktualisieren ausführen. Sie können auch UpdateServiceoder verwenden AWS CLI.

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbeh ebung
		• Wurde die Aufgabe gestartet, nachdem der ECS-Cluster von Runtime Monitoring ausgeschlossen wurde? Wenn Sie das vordefinierte GuardDuty Tag von `GuardDuty Managed` - in - `true` ändern`false`, GuardDuty werden die Runtime-E reignisse für den ECS-Cluster nicht empfangen. `GuardDutyManaged` • Fehlt Ihrer Aufgabe eine? `TaskExecu tionRole` Das Hinzufügen von a ist obligator isch, `TaskExecutionRole` da GuardDuty Berechtigungen zum Herunterladen des GuardDuty Containers aus dem ECR-Repository erforderlich sind. Weitere Informati onen finden Sie unter Geben Sie ECR-Berechtigungen und Subnetzde tails an. • Enthält Ihr Service eine Aufgabe, die das alte Format von `taskArn` hat? GuardDuty Runtime Monitoring unterstützt die Abdeckung von Aufgaben nicht, die das alte Format von haben`taskArn`. Informationen zu Amazon Resource Names (ARNs) für Amazon ECS-

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbeh ebung
		Ressourcen finden Sie unter Amazon Resource Names (ARNs) and IDs.

Abdeckung für Amazon EKS-Cluster

Nachdem Sie Runtime Monitoring aktiviert und den GuardDuty Security Agent (Add-on) für EKS entweder manuell oder über die automatische Agentenkonfiguration installiert haben, können Sie mit der Bewertung der Abdeckung Ihrer EKS-Cluster beginnen.

Inhalt

Überprüfen der Abdeckungsstatistiken

Die Abdeckungsstatistiken für die EKS-Cluster, die Ihren eigenen Konten oder Ihren Mitgliedskonten zugeordnet sind, geben den Prozentsatz der fehlerfreien EKS-Cluster an allen EKS-Clustern in der ausgewählten AWS-Region an. Die folgende Gleichung stellt dies wie folgt dar:

(Fehlerfreie Cluster/Alle Cluster)*100

Wählen Sie eine der Zugriffsmethoden, um die Abdeckungsstatistiken für Ihre Konten einzusehen.

Console

- Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
- Wählen Sie im Navigationsbereich Runtime Monitoring aus.
- Wählen Sie die Registerkarte Laufzeitabdeckung von EKS-Clustern.
- Auf der Registerkarte Laufzeitabdeckung von EKS-Clustern können Sie die Abdeckungsstatistiken einsehen, die nach dem Abdeckungsstatus aggregiert sind, der in der Cluster-Listentabelle verfügbar ist.
  - Sie können die Tabelle mit der Cluster-Liste nach den folgenden Spalten filtern:

    - Cluster name
    - Konto-ID
    - Agentenverwaltungs-Typ
    - Abdeckungsstatus
    - Add-On-Version
- Wenn einer Ihrer EKS-Cluster den Abdeckungsstatus Fehlerhaft hat, kann die Spalte Problem zusätzliche Informationen über den Grund für den Status Fehlerhaft enthalten.

API/CLI

- Führen Sie die ListCoverageAPI mit Ihrer eigenen gültigen Detektor-ID, Region und Ihrem Service-Endpunkt aus. Mit dieser API können Sie die Cluster-Liste filtern und sortieren.
    - Sie können das Beispiel `filter-criteria` ändern mit einer der folgenden Optionen für `CriterionKey`:
        - `ACCOUNT_ID`
        - `CLUSTER_NAME`
        - `RESOURCE_TYPE`
        - `COVERAGE_STATUS`
        - `ADDON_VERSION`
        - `MANAGEMENT_TYPE`
    - Sie können das Beispiel `AttributeName` in `sort-criteria` ändern mit einer der folgenden Optionen:
        - `ACCOUNT_ID`
        - `CLUSTER_NAME`
        - `COVERAGE_STATUS`
        - `ISSUE`
        - `ADDON_VERSION`
        - `UPDATED_AT`
    - Sie können *`max-results`* ändern (bis zu 50).
    - Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ - Konsole.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Führen Sie die GetCoverageStatisticsAPI aus, um aggregierte Statistiken zur Abdeckung abzurufen, die `statisticsType` auf dem basieren.
  - Sie können das Beispiel `statisticsType` zu einer der folgenden Optionen ändern:
    - `COUNT_BY_COVERAGE_STATUS` – Stellt Abdeckungsstatistiken für EKS-Cluster dar, aggregiert nach Abdeckungs-Status.
    - `COUNT_BY_RESOURCE_TYPE`— Statistiken zur Abdeckung, aggregiert auf der Grundlage des AWS Ressourcentyps in der Liste.
    - Sie können das Beispiel `filter-criteria` im Befehl ändern. Sie können die folgenden Optionen für `CriterionKey` verwenden:
      - `ACCOUNT_ID`
      - `CLUSTER_NAME`
      - `RESOURCE_TYPE`
      - `COVERAGE_STATUS`
      - `ADDON_VERSION`
      - `MANAGEMENT_TYPE`
  - Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ - Konsole.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Wenn der Abdeckungsstatus Ihres EKS-Clusters Fehlerhaft ist, finden Sie weitere Informationen unter Behebung von Problemen mit der EKS-Abdeckung.

Benachrichtigungen über Änderungen des Abdeckungsstatus konfigurieren

Der Abdeckungsstatus eines EKS-Clusters in Ihrem Konto wird möglicherweise als Fehlerhaft angezeigt. Um zu erkennen, wann der Abdeckungsstatus Fehlerhaft wird, empfehlen wir Ihnen, den Abdeckungsstatus regelmäßig zu überwachen und Fehler zu beheben, falls der Status Fehlerhaft ist. Alternativ können Sie eine EventBridge Amazon-Regel erstellen, die Sie benachrichtigt, wenn sich der Deckungsstatus von einem `Unhealthy` auf `Healthy` oder einem anderen Wert ändert. GuardDuty Veröffentlicht dies standardmäßig im EventBridgeBus für Ihr Konto.

Beispiel für ein Benachrichtigungsschema

In einer EventBridge Regel können Sie die vordefinierten Beispielereignisse und Ereignismuster verwenden, um Benachrichtigungen über den Versicherungsstatus zu erhalten. Weitere Informationen zum Erstellen einer EventBridge Regel finden Sie unter Regel erstellen im EventBridge Amazon-Benutzerhandbuch.

Darüber hinaus können Sie mithilfe des folgenden Beispiel-Benachrichtigungsschemas ein benutzerdefiniertes Ereignismuster erstellen. Achten Sie darauf, die Werte für Ihr Konto zu ersetzen. Um benachrichtigt zu werden, wenn sich der Abdeckungsstatus Ihres Amazon EKS-Clusters von `Healthy` zu ändert`Unhealthy`, `detail-type` sollte *`GuardDuty Runtime Protection Unhealthy lauten`*. Um benachrichtigt zu werden, wenn sich der Deckungsstatus von `Unhealthy` auf ändert`Healthy`, ersetzen Sie den Wert von `detail-type` durch *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS-Konto ID",
  "time": "event timestamp (string)",
  "region": "AWS-Region",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EKS",
```

```
        "eksClusterDetails": {
            "clusterName": "string",
            "availableNodes": "string",
             "desiredNodes": "string",
             "addonVersion": "string"
         }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Behebung von Problemen mit der EKS-Abdeckung

Wenn der Abdeckungsstatus für Ihren EKS-Cluster lautet`Unhealthy`, können Sie den entsprechenden Fehler entweder in der Spalte Problem in der GuardDuty Konsole oder mithilfe des CoverageResourceDatentyps anzeigen.

Wenn Sie mit Einschluss- oder Ausschluss-Tags arbeiten, um Ihre EKS-Cluster selektiv zu überwachen, kann es einige Zeit dauern, bis die Tags synchronisiert sind. Dies kann sich auf den Abdeckungsstatus des zugehörigen EKS-Clusters auswirken. Sie können erneut versuchen, das entsprechende Tag (Einschluss oder Ausschluss) zu entfernen und hinzuzufügen. Weitere Informationen finden Sie unter Markieren Ihrer Amazon-EKS-Ressourcen im Amazon-EKS-Entwicklerhandbuch.

Die Struktur eines Abdeckungsproblems ist `Issue type:Extra information`. In der Regel verfügen die Probleme über optionale Zusatzinformationen, die eine spezifische Ausnahme oder eine Beschreibung des Problems enthalten können. Basierend auf zusätzlichen Informationen enthalten die folgenden Tabellen die empfohlenen Schritte zur Behebung von Deckungsproblemen für Ihre EKS-Cluster.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
Die Erstellung des Addons ist fehlgeschlagen	Das Addon `aws-guardduty-agent` ist mit der aktuellen Clusterversion des Clusters nicht kompatibel. *`ClusterNa`*	Stellen Sie sicher, dass Sie eine der Kubernetes-Versionen verwenden, die die Bereitstellung des `aws-guardduty-`

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
	me Das angegebene Add-On wird nicht unterstützt.	`agent` -EKS-Add-Ons unterstützen. Weitere Informationen finden Sie unter Kubernetes-Versionen, die vom Security Agent unterstützt werden GuardDuty . Informationen zur Aktualisierung Ihrer Kubernetes-Version finden Sie unter Aktualisieren einer Amazon-EKS-Cluster-Kubernetes-Version.
Die Erstellung des Addons ist fehlgeschlagen Die Aktualisierung des Addons ist fehlgeschlagen Der Status des Addons ist fehlerhaft	Problem mit dem EKS-Add-On – `AddonIssueCode` : `AddonIssueMessage`	Informationen zu empfohlenen Schritten für einen bestimmten Problemcode eines Add-ons finden Sie unter. Troubleshooting steps for Addon creation/updatation error with Addon issue code Eine Liste der Addon-Problemcodes, die bei diesem Problem auftreten können, finden Sie unter AddonIssue.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
VPC-Endpunkterstellung ist fehlgeschlagen	*VPC-Endpunkterstellung wird für gemeinsam genutzte VPC-VPCid nicht unterstützt*	Runtime Monitoring unterstützt jetzt die Verwendung einer gemeinsam genutzten VPC innerhalb einer Organisation. Stellen Sie sicher, dass Ihre Konten alle Voraussetzungen erfüllen. Weitere Informationen finden Sie unter Voraussetzungen für die Verwendung von Shared VPC.
	Nur bei Verwendung einer gemeinsam genutzten VPC mit automatisierter Agentenkonfiguration Die Besitzerkonto-ID *111122223333* für gemeinsam genutzte *VPC-vPCid* hat weder Runtime Monitoring noch automatische Agentenkonfiguration oder beides aktiviert.	Das gemeinsame VPC-Besitzerkonto muss Runtime Monitoring und automatische Agentenkonfiguration für mindestens einen Ressourcentyp (Amazon EKS oder Amazon ECS (AWS Fargate)) aktivieren. Weitere Informationen finden Sie unter Spezifische Voraussetzungen für Runtime Monitoring GuardDuty.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
	Um privates DNS zu aktivieren, müssen sowohl das enableDnsSupport - als auch das enableDnsHostnames -VPC-Attribute für vpcId auf true gesetzt sein (Service: Ec2, Status Code:400, Request ID: a1b2c3d4-5678-90ab-cdef-EXAMPLE11111).	Sie müssen jedoch sicherstellen, dass die folgenden VPC-Attribute auf `true` festgelegt sind: `enableDnsSupport` und `enableDns Hostnames` . Weitere Informationen finden Sie unter DNS-Attribute in Ihrer VPC. Wenn Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/ verwenden , um die Amazon VPC zu erstellen, stellen Sie sicher, dass Sie sowohl DNS-Hostnamen aktivieren als auch DNS-Auflösung aktivieren auswählen. Weitere Informationen finden Sie unter VPC-Konfigurationsoptionen.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
Fehler beim Löschen eines gemeinsamen VPC-Endpunkts	*Das Löschen eines gemeinsamen VPC-Endpunkts ist für die Konto-ID 111122223333 , die gemeinsame VPC-VPC-ID , die Besitzerkonto-ID 5555555555 nicht zulässig.*	Mögliche Schritte: • Die Deaktivierung des Runtime Monitoring-Status des gemeinsam genutzten VPC-Teilnehmerkontos hat keine Auswirkungen auf die gemeinsame VPC-Endpunktrichtlinie und die Sicherheitsgruppe, die im Besitzerkonto vorhanden ist. Um den gemeinsamen VPC-Endpunkt und die Sicherheitsgruppe zu löschen, müssen Sie Runtime Monitoring oder den Status der automatisierten Agentenkonfiguration im gemeinsam genutzten VPC-Besitzerkonto deaktivieren. • Das gemeinsame VPC-Teilnehmerkonto kann den gemeinsamen VPC-Endpunkt und die Sicherheitsgruppe, die im gemeinsamen VPC-Besitzerkonto gehostet werden, nicht löschen.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
Lokale EKS-Cluster	EKS-Add-Ons werden auf lokalen Outpost-Clustern nicht unterstützt.	Nicht umsetzbar. Weitere Informationen finden Sie unter Amazon EKS in AWS Outposts.
Die Aktivierungsberechtigung für die EKS-Laufzeit-Überwachung wurde nicht erteilt	(kann zusätzliche Informationen anzeigen oder auch nicht)	1. Wenn die zusätzlichen Informationen für dieses Problem verfügbar sind, beheben Sie die Ursache und folgen Sie dem nächsten Schritt. 2. Schalten Sie die EKS-Laufzeit-Überwachung aus und dann wieder ein. Stellen Sie sicher, dass der GuardDuty Agent ebenfalls bereitgestellt wird, sei es automatisch GuardDuty oder manuell.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
Die Bereitstellung der Ressourcen zur Aktivierung der EKS-Laufzeit-Überwachung wird ausgeführt	(kann zusätzliche Informationen anzeigen oder auch nicht)	Nicht umsetzbar. Nachdem Sie die EKS-Laufzeit-Überwachung aktiviert haben, kann der Abdeckungsstatus `Unhealthy` bleiben, bis der Schritt der Ressourcenbereitstellung abgeschlossen ist. Der Abdeckungsstatus wird regelmäßig überwacht und aktualisiert.
Andere (jedes andere Problem)	Fehler aufgrund eines Autorisierungsfehlers	Schalten Sie die EKS-Laufzeit-Überwachung aus und dann wieder ein. Stellen Sie sicher, dass der GuardDuty Agent ebenfalls bereitgestellt wird, entweder automatisch GuardDuty oder manuell.

Fehler bei der Erstellung oder Aktualisierung des Addons	Fehlerbehebungsschritte
Problem mit dem EKS-Addon - `InsufficientNumberOfReplicas` : Das Add-on ist fehlerhaft, da es nicht über die gewünschte Anzahl von Replikaten verfügt.	Mithilfe der Problemmeldung können Sie die Ursache identifizieren und beheben. Sie können damit beginnen, Ihren Cluster zu beschreiben. Verwenden Sie dies beispiels

Fehler bei der Erstellung oder Aktualisierung des Addons	Fehlerbehebungsschritte
	weise, `kubectl describe pods` um die Hauptursache für den Pod-Ausfall zu ermitteln. Nachdem Sie die Ursache behoben haben, wiederholen Sie den Schritt (Erstellung oder Aktualisierung des Add-ons).
EKS Addon Issue —`AdmissionRequestDenied` : Der Zugangswebhook `"validate.kyverno.svc-fail"` hat die Anfrage abgelehnt: Richtlinie `DaemonSet/amazon-guardduty/aws-guardduty-agent` wegen Ressourcenverletzung:::... restrict-image-registries `autogen-validate-registries`	1. Der Amazon EKS-Cluster oder der Sicherheitsadministrator müssen die Sicherheitsrichtlinie überprüfen, die das Addon-Update blockiert. 2. Sie müssen entweder den Controller (`webhook`) deaktivieren oder den Controller die Anfragen von Amazon EKS annehmen lassen.
Problem mit dem EKS-Addon `ConfigurationConflict` — Beim Versuch, sich zu bewerben, wurden Konflikte festgestellt. Wird aufgrund des Konfliktlösungsmodus nicht fortgesetzt. `Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.template.spec.containers[name="aws-guardduty-agent"].image`	Wenn Sie das Addon erstellen oder aktualisieren, geben Sie das `OVERWRITE` Konfliktlösungskennzeichen an. Dadurch werden möglicherweise alle Änderungen überschrieben, die mithilfe der Kubernetes-API direkt an den zugehörigen Ressourcen in Kubernetes vorgenommen wurden. Sie können das Addon zuerst löschen und dann erneut installieren.

Fehler bei der Erstellung oder Aktualisierung des Addons	Fehlerbehebungsschritte

Problem mit dem EKS-Addon - `AccessDenied: priorityclasses.scheduling.k8s.io "aws-guardduty-agent.priorityclass" is forbidden: User "eks:addon-manager" cannot patch resource "priorityclasses" in API group "scheduling.k8s.io" at the cluster scope`	Sie müssen die fehlende Berechtigung `eks:addon-cluster-admin ClusterRoleBinding` manuell hinzufügen. Fügen Sie Folgendes `yaml` hinzu`eks:addon-cluster-admin` :
	
	`---`
	`kind: ClusterRoleBinding`
	`apiVersion: rbac.authorization.k8s.io/v1`
	`metadata:`
	`  name: eks:addon-cluster-admin`
	`subjects:`
	`- kind: User`
	`  name: eks:addon-manager`
	`  apiGroup: rbac.authorization.k8s.io`
	`roleRef:`
	`  kind: ClusterRole`
	`  name: cluster-admin`
	`  apiGroup: rbac.authorization.k8s.io`
	`---`
	
	Sie können dies jetzt mit `yaml` dem folgenden Befehl auf Ihren Amazon EKS-Cluster anwenden:
	
	`kubectl apply -f eks-addon-cluster-admin.yaml`

Fehler bei der Erstellung oder Aktualisierung des Addons	Fehlerbehebungsschritte
Problem mit dem EKS-Addon - `AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label`	Sie müssen entweder den Controller deaktivieren oder den Controller die Anfragen vom Amazon EKS-Cluster annehmen lassen. Bevor Sie das Add-on erstellen oder aktualisieren, können Sie auch einen GuardDuty Namespace erstellen und ihn als `owner` kennzeichnen.

Häufig gestellte Fragen (FAQ)

Inhalt

Warum ist meine Ressource immer noch abgedeckt, **`Unhealthy`** obwohl Runtime Monitoring aktiviert, der GuardDuty Security Agent installiert und alle Voraussetzungen erfüllt sind?

Wenn Sie den GuardDuty Security Agent gerade installiert haben (entweder über die automatische Agentenkonfiguration oder manuell) oder die empfohlenen Schritte zur Behebung eines Deckungsproblems befolgt haben, kann es einige Minuten dauern, bis der Schutzstatus wieder fehlerfrei ist. Sie können den Deckungsstatus entweder regelmäßig überprüfen oder Amazon EventBridge (EventBridge) so konfigurieren, dass Sie eine Benachrichtigung erhalten, wenn sich der Deckungsstatus ändert.

Wer kann den Status der Runtime-Abdeckung einer Ressource einsehen, die mir gehört AWS-Konto?

Als Mitgliedskonto oder eigenständiges Konto können Sie die Deckungsstatistiken der Ressourcen einsehen, die Ihren eigenen Konten zugeordnet sind. Als delegiertes GuardDuty Administratorkonto einer Organisation können Sie die Deckungsstatistiken für die mit Ihrem Konto verknüpften Ressourcen und die Mitgliedskonten, die zu Ihrer Organisation gehören, einsehen.

Einrichten der CPU- und Arbeitsspeicherüberwachung

Nachdem Sie Runtime Monitoring aktiviert und festgestellt haben, dass der Abdeckungsstatus Ihres Clusters fehlerfrei ist, können Sie die Insight-Metriken einrichten und anzeigen.

Mithilfe der folgenden Themen können Sie beurteilen, wie der bereitgestellte Agent im Vergleich zu den CPU- und Speicherlimits für den GuardDuty Agenten abschneidet.

Überwachung auf dem Amazon ECS-Cluster einrichten

Mithilfe der folgenden Schritte aus dem CloudWatch Amazon-Benutzerhandbuch können Sie beurteilen, wie der bereitgestellte Agent im Vergleich zu den CPU- und Speicherlimits für den GuardDuty Agenten abschneidet:

1. Einrichtung von Container Insights auf Amazon ECS für Metriken auf Cluster- und Service-Ebene
2. Amazon ECS Container Insights-Metriken

Überwachung auf dem Amazon EKS-Cluster einrichten

Nachdem der GuardDuty Security Agent bereitgestellt wurde und Sie festgestellt haben, dass der Schutzstatus Ihres Clusters fehlerfrei ist, können Sie die Container Insight-Metriken einrichten und anzeigen.

Bewerten Sie die Leistung des Security Agents

1. Einrichtung von Container Insights auf Amazon EKS und Kubernetes im Amazon-Benutzerhandbuch CloudWatch
2. Kennzahlen zu Amazon EKS und Kubernetes Container Insights im Amazon-Benutzerhandbuch CloudWatch

Verwalten Sie die Leistung mit dem Security Agent v1.5.0 und höher

Bei Security Agent v1.5.0 und höher können Sie bestimmte Parameter konfigurieren, wenn die Erkenntnisse darauf hindeuten, dass der zugehörige GuardDuty Agent die zugewiesenen Grenzwerte erreicht. Weitere Informationen finden Sie unter Konfigurieren Sie die EKS-Zusatzparameter.

Gesammelte Runtime-Ereignistypen, die verwendet GuardDuty

Der GuardDuty Security Agent sammelt die folgenden Ereignistypen und sendet sie zur Erkennung und Analyse von Bedrohungen an das GuardDuty Backend. GuardDuty macht Ihnen diese Ereignisse nicht zugänglich. Wenn eine potenzielle Bedrohung GuardDuty erkannt und ein Runtime Monitoring-Ergebnis generiert wird, können Sie die entsprechenden Ergebnisdetails einsehen. Weitere Hinweise zur GuardDuty Verwendung der gesammelten Ereignistypen finden Sie unterAbmeldung von der Verwendung Ihrer Daten zur Serviceverbesserung.

Ereignisse verarbeiten

Feldname	Beschreibung
Prozessname	Name des beobachteten Prozesses.
Prozesspfad	Absoluter Pfad der ausführbaren Datei des Prozesses.
Prozess-ID	Die ID, die dem Prozess vom Betriebssystem zugewiesen wurde.
Namespace-PID	Die Prozess-ID des Prozesses in einem sekundären PID-Namespace, bei dem es sich nicht um den PID-Namespace auf Host-Ebene handelt. Bei Prozessen innerhalb eines Containers ist dies die Prozess-ID, die innerhalb des Containers beobachtet wird.
Prozess-Benutzer-ID	Die eindeutige ID des Benutzers, der den Prozess ausgeführt hat.

Feldname	Beschreibung
Prozess-UUID	Die eindeutige ID, die dem Prozess von zugewiesen wurde GuardDuty.
Prozess-GID	Prozess-ID der Prozessgruppe.
Prozess-EGID	Effektive Gruppen-ID der Prozessgruppe.
Prozess-EUID	Effektive Benutzer-ID des Prozesses.
Prozess-Benutzername	Der Benutzername, der den Prozess ausgeführt hat.
Prozesses-Startzeit	Die Zeit, zu der der Prozess erstellt wurde. Dieses Feld hat das UTC-Datums-Zeichenfolgenformat (`2023-03-22T19:37:20.168Z`).
Ausführbare Prozessdatei SHA-256	Der Hash `SHA256` der ausführbaren Prozessesdatei.
Prozess-Skriptpfad	Pfad der Skriptdatei, die ausgeführt wurde.
Prozess-Umgebungsvariable	Die Umgebungsvariable, die dem Prozess zur Verfügung gestellt wurde. Nur `LD_PRELOAD` und `LD_LIBRARY_PATH` werden gesammelt.
Aktuelles Arbeitsverzeichnis (PWD) des Prozesses	Derzeitiges Arbeitsverzeichnis des Prozesses.
Übergeordneter Prozess	Prozessdetails des übergeordneten Prozesses. Ein übergeordneter Prozess ist ein Prozess, der den beobachteten Prozess erzeugt hat.

Feldname	Beschreibung
Befehlszeilenargumente Derzeit ist dieses Feld auf bestimmte Agentenversionen beschränkt, die dem Ressourcentyp entsprechen: • Fargate (nur Amazon ECS) mit GuardDuty Security Agent v1.0.0 und höher. • Amazon EC2 EC2-Instances mit GuardDuty Security Agent v1.0.0 und höher. • Amazon EKS-Cluster mit Security Agent v1.4.0 und höher. Weitere Informationen finden Sie unter GuardDuty Versionsverlauf des Agenten.	Befehlszeilenargumente, die zum Zeitpunkt der Prozessausführung bereitgestellt wurden. Dieses Feld kann vertrauliche Kundendaten enthalten.

Container-Ereignisse

Feldname	Beschreibung
Container-Name	Name des Containers. Falls verfügbar, zeigt dieses Feld den Wert des Labels `io.kubenetes.container.name` an.
Container-UID	Die eindeutige ID des Containers, die von der Container-Laufzeit zugewiesen wurde.
Container-Laufzeit	Die Container-Laufzeit (wie z. B. `docker` oder `containerd`), die zum Ausführen des Containers verwendet wurde.
Container-Image-ID	Die ID des Container-Images.
Container-Image-Name	Name des Container-Images.

AWS Fargate (nur Amazon ECS) Aufgabenereignisse

Feldname	Beschreibung
Amazon-Ressourcenname (ARN) der Aufgabe	Der ARN der Aufgabe.
Cluster-Name	Der Name des Amazon ECS-Clusters.
Familienname	Der Familienname der Aufgabendefinition. Der `family` wird als Name für die Aufgabendefinition verwendet, mit der die Aufgabe gestartet wird.
Service-Name	Der Name des Amazon ECS-Service, wenn die Aufgabe als Teil eines Services gestartet wurde.
Starttyp	Die Infrastruktur, auf der Ihre Aufgabe ausgeführt wird. Für Runtime Monitoring mit dem Ressourcentyp as `ECSCluster` kann der Starttyp entweder `EC2` oder sein`FARGATE`.
CPU	Die Anzahl der von der Aufgabe verwendeten CPU-Einheiten, wie in der Aufgabendefinition angegeben.

Kubernetes-Pod-Ereignisse

Feldname	Beschreibung
Pod-ID	Die ID des Kubernetes-Pods.
Pod-Name	Name des Kubernetes-Pods.
Pod-Namespace	Name des Kubernetes-Namespace, zu dem der Kubernetes-Workload gehört.
Kubernetes-Cluster-Name	Name des Kubernetes-Clusters.

DNS-Ereignisse

Feldname	Beschreibung
Socket-Typ	Socket-Typ zur Angabe der Kommunikationssemantik. z. B. `SOCK_RAW`.
Adress-Familie	Stellt das der Adresse zugeordnete Kommunikationsprotokoll dar. Die Adressfamilie `AF_INET` wird beispielsweise für das IP-v4-Protokoll verwendet.
Richtungs-ID	Die ID der Verbindungsrichtung.
Protokollnummer	Die Layer-4-Protokollnummer, z. B. 17 für UDP und 6 für TCP.
DNS-Remote-Endpunkt-IP	Die Remote-IP-Informationen der Verbindung.
DNS-Remote-Endpunkt-Port	Die Portnummer der Verbindung.
Lokale DNS-Endpunkt-IP	Die lokale IP der Verbindung.
Lokaler DNS-Endpunkt-Port	Die Portnummer der Verbindung.
DNS-Nutzlast	Die Nutzlast von DNS-Paketen, die DNS-Abfragen und -Antworten enthalten.

Offene Ereignisse

Feldname	Beschreibung
Dateipfad	Pfad der Datei, die in diesem Ereignis geöffnet wird.
Flags	Beschreibt den Dateizugriffsmodus, z. B. Schreibgeschützt, Nur-Schreiben und Lesen-Schreiben.

Lastmodul-Ereignis

Feldname	Beschreibung
Modulname	Name des in den Kernel geladenen Moduls.

Mprotect-Ereignisse

Feldname	Beschreibung
Adressbereiche	Der Adressbereich, für den der Zugriffsschutz geändert wurde.
Arbeitsspeicherregionen	Gibt die Region des Adressraums eines Prozesses an, z. B. Stapel und Heap.
Flags	Stellt Optionen dar, die das Verhalten dieses Ereignisses steuern.

Mount-Ereignisse

Feldname	Beschreibung
Mount-Ziel	Der Pfad, in dem die Mount-Quelle gemountet ist.
Mount-Quelle	Der Pfad auf dem Host, der am Mount-Ziel gemountet ist.
Typ des Dateisystems	Repräsentiert den Typ des bereitgestellten Dateisystems.
Flags	Stellt Optionen dar, die das Verhalten dieses Ereignisses steuern.

Verknüpfungs-Ereignisse

Feldname	Beschreibung
Verknüpfungs-Pfad	Pfad, in dem der Hardlink erstellt wird.
Zielpfad	Pfad der Datei, auf die der Hardlink verweist.

Symlink-Ereignisse

Feldname	Beschreibung
Verknüpfungs-Pfad	Pfad, in dem der symbolische Link erstellt wird.
Zielpfad	Pfad der Datei, auf die der symbolische Link verweist.

Dup-Ereignisse

Feldname	Beschreibung
Alter Dateideskriptor	Ein Dateideskriptor, der ein geöffnetes Dateiobjekt darstellt.
Neuer Dateideskriptor	Ein neuer Dateideskriptor, der ein Duplikat des alten Dateidesk riptors ist. Sowohl der alte als auch der neue Dateideskriptor stehen für dasselbe offene Dateiobjekt.
DNS-Remote-Endpunkt-IP	Die Remote-IP-Adresse des Netzwerk-Sockets, dargestel lt durch den alten Dateideskriptor. Gilt nur, wenn der alte Dateideskriptor einen Netzwerk-Socket darstellt.
DNS-Remote-Endpunkt-Port	Die Remote-IP-Adresse des Netzwerk-Sockets, dargestel lt durch den alten Dateideskriptor. Gilt nur, wenn der alte Dateideskriptor einen Netzwerk-Socket darstellt.

Feldname	Beschreibung
Lokale Dup-Endpunkt-IP	Die lokale IP-Adresse des Netzwerk-Sockets, dargestellt durch den alten Dateideskriptor. Gilt nur, wenn der alte Dateideskriptor einen Netzwerk-Socket darstellt.
Lokaler Dup-Endpunkt-Port	Der lokale Port des Netzwerk-Sockets, dargestellt durch den alten Dateideskriptor. Gilt nur, wenn der alte Dateideskriptor einen Netzwerk-Socket darstellt.

Arbeitsspeicherzuordnungs-Ereignis

Feldname	Beschreibung
Dateipfad	Pfad der Datei, der der Arbeitsspeicher zugeordnet ist.

Socket-Ereignisse

Feldname	Beschreibung
Adress-Familie	Stellt das der Adresse zugeordnete Kommunikationsprotokoll dar. Die Adressfamilie `AF_INET` wird beispielsweise für das IP-v4-Protokoll verwendet.
Socket-Typ	Socket-Typ zur Angabe der Kommunikationssemantik. z. B. `SOCK_RAW`.
Protokollnummer	Spezifiziert ein bestimmtes Protokoll innerhalb der Adressfam ilie. Normalerweise gibt es ein einziges Protokoll in Adressfam ilien. Beispielsweise hat die Adressfamilie `AF_INET` nur das IP-Protokoll.

Verbindungs-Ereignisse

Feldname	Beschreibung
Adress-Familie	Stellt das der Adresse zugeordnete Kommunikationsprotokoll dar. Die Adressfamilie `AF_INET` wird beispielsweise für das IP-v4-Protokoll verwendet.
Socket-Typ	Socket-Typ zur Angabe der Kommunikationssemantik. z. B. `SOCK_RAW`.
Protokollnummer	Spezifiziert ein bestimmtes Protokoll innerhalb der Adressfam ilie. Normalerweise gibt es ein einziges Protokoll in Adressfam ilien. Beispielsweise hat die Adressfamilie `AF_INET` nur das IP-Protokoll.
Dateipfad	Pfad der Socket-Datei, falls die Adressfamilie `AF_UNIX` ist.
Remote-Endpunkt-IP	Die Remote-IP-Informationen der Verbindung.
Remote-Endpunkt-Port	Die Portnummer der Verbindung.
Lokale Endpunkt-IP	Die lokale IP der Verbindung.
Lokaler Endpunkt-Port	Die Portnummer der Verbindung.

Prozess-VM-Readv-Ereignisse

Feldname	Beschreibung
Flags	Stellt Optionen dar, die das Verhalten dieses Ereignisses steuern.
Ziel-PID	Prozess-ID des Prozesses, aus dessen Arbeitsspeicher gelesen wird.
UUID des Zielprozesses	Die eindeutige ID des Zielprozesses.

Feldname	Beschreibung
Pfad der ausführbaren Zieldatei	Absoluter Pfad der ausführbaren Zieldatei des Prozesses.

Prozess-VM-Writev-Ereignisse

Feldname	Beschreibung
Flags	Stellt Optionen dar, die das Verhalten dieses Ereignisses steuern.
Ziel-PID	Prozess-ID des Prozesses, in den Arbeitsspeicher geschrieben wird.
UUID des Zielprozesses	Die eindeutige ID des Zielprozesses.
Pfad der ausführbaren Zieldatei	Absoluter Pfad der ausführbaren Zieldatei des Prozesses.

Ptrace-Ereignisse

Feldname	Beschreibung
Ziel-PID	Prozess-ID des Zielprozesses.
UUID des Zielprozesses	Die eindeutige ID des Zielprozesses.
Pfad der ausführbaren Zieldatei	Absoluter Pfad der ausführbaren Zieldatei des Prozesses.
Flags	Stellt Optionen dar, die das Verhalten dieses Ereignisses steuern.

Ereignisse binden

Feldname	Beschreibung
Adress-Familie	Stellt das der Adresse zugeordnete Kommunikationsprotokoll dar. Die Adressfamilie `AF_INET` wird beispielsweise für das IP-v4-Protokoll verwendet.
Socket-Typ	Socket-Typ zur Angabe der Kommunikationssemantik. z. B. `SOCK_RAW`.
Protokollnummer	Die Layer-4-Protokollnummer, z. B. 17 für UDP und 6 für TCP.
Lokale Endpunkt-IP	Die lokale IP der Verbindung.
Lokaler Endpunkt-Port	Die Portnummer der Verbindung.

Ereignisse abhören

Feldname	Beschreibung
Adress-Familie	Stellt das der Adresse zugeordnete Kommunikationsprotokoll dar. Die Adressfamilie `AF_INET` wird beispielsweise für das IP-v4-Protokoll verwendet.
Socket-Typ	Socket-Typ zur Angabe der Kommunikationssemantik. z. B. `SOCK_RAW`.
Protokollnummer	Die Layer-4-Protokollnummer, z. B. 17 für UDP und 6 für TCP.
Lokale Endpunkt-IP	Die lokale IP der Verbindung.
Lokaler Endpunkt-Port	Die Portnummer der Verbindung.

Ereignisse umbenennen

Feldname	Beschreibung
Dateipfad	Pfad, in dem die Datei umbenannt wurde.
Ziel	Der neue Pfad der Datei.

Legen Sie UID-Ereignisse fest

Feldname	Beschreibung
Neue EUID	Die neue effektive Benutzer-ID des Prozesses.
Neue UID	Die neue Benutzer-ID des Prozesses.

Chmod-Ereignisse

Feldname	Beschreibung
Dateipfad	Pfad der Datei, die dieses Ereignis auslöst.
Dateimodus	Die aktualisierten Zugriffsberechtigungen für die zugehörige Datei.

GuardDuty Hosting-Agent für Amazon ECR Repositorys

In den folgenden Abschnitten sind die Amazon Elastic Container Registry (Amazon ECR) - Repositorys aufgeführt, in denen der Sicherheitsagent GuardDuty gehostet wird, der auf Ihren Amazon EKS- und Amazon ECS-Clustern bereitgestellt wird.

Inhalt

Repository für EKS Agent Version 1.6.0 oder höher

Die folgende Tabelle zeigt die Amazon ECR-Repositorys, die jeweils den Amazon EKS-Add-On-Agenten der Version (`aws-guardduty-agent`) 1.6.0 und höher hosten. AWS-Region

AWS-Region	Amazon-ECR-Repository-URI
USA West (Oregon)	`602401143452.dkr.ecr.us-west-2.amazonaws.com`
Europa (Paris)	`602401143452.dkr.ecr.eu-west-3.amazonaws.com`
Asien-Pazifik (Mumbai)	`602401143452.dkr.ecr.ap-south-1.amazonaws.com`
Asien-Pazifik (Hyderabad)	`900889452093.dkr.ecr.ap-south-2.amazonaws.com`
Kanada (Zentral)	`602401143452.dkr.ecr.ca-central-1.amazonaws.com`
Kanada West (Calgary)	`761377655185.dkr.ecr.ca-west-1.amazonaws.com`
Naher Osten (VAE)	`759879836304.dkr.ecr.me-central-1.amazonaws.com`
Europe (London)	`602401143452.dkr.ecr.eu-west-2.amazonaws.com`
Europa (Irland)	`602401143452.dkr.ecr.us-west-1.amazonaws.com`
USA Ost (Nord-Virginia)	`602401143452.dkr.ecr.us-east-1.amazonaws.com`
USA Ost (Ohio)	`602401143452.dkr.ecr.us-east-2.amazonaws.com`
Europa (Irland)	`602401143452.dkr.ecr.eu-west-1.amazonaws.com`
Südamerika (São Paulo)	`602401143452.dkr.ecr.sa-east-1.amazonaws.com`

AWS-Region	Amazon-ECR-Repository-URI
Europa (Stockholm)	602401143452.dkr.ecr.eu-north-1.amazonaws.com
Europa (Frankfurt)	602401143452.dkr.ecr.eu-central-1.amazonaws.com
Europa (Zürich)	900612956339.dkr.ecr.eu-central-2.amazonaws.com
Asien-Pazifik (Singapur)	602401143452.dkr.ecr.ap-southeast-1.amazonaws.com
Asien-Pazifik (Sydney)	602401143452.dkr.ecr.ap-southeast-2.amazonaws.com
Asien-Pazifik (Jakarta)	296578399912.dkr.ecr.ap-southeast-3.amazonaws.com
Asien-Pazifik (Tokio)	602401143452.dkr.ecr.ap-northeast-1.amazonaws.com
Asien-Pazifik (Seoul)	602401143452.dkr.ecr.ap-northeast-2.amazonaws.com
Asien-Pazifik (Osaka)	602401143452.dkr.ecr.ap-northeast-3.amazonaws.com
Asien-Pazifik (Hongkong)	800184023465.dkr.ecr.ap-east-1.amazonaws.com
Naher Osten (Bahrain)	759879836304.dkr.ecr.me-south-1.amazonaws.com
Europa (Milan)	590381155156.dkr.ecr.eu-south-1.amazonaws.com
Europa (Spain)	455263428931.dkr.ecr.eu-south-2.amazonaws.com
Afrika (Kapstadt)	877085696533.dkr.ecr.af-south-1.amazonaws.com

AWS-Region	Amazon-ECR-Repository-URI
Asien-Pazifik (Melbourne)	`491585149902.dkr.ecr.ap-southeast-4.amazonaws.com`
Israel (Tel Aviv)	`066635153087.dkr.ecr.il-central-1.amazonaws.com`

Repository für EKS Agent Version 1.5.0 und früher

In der folgenden Tabelle sind die Amazon ECR-Repositorys aufgeführt, die jeweils den Amazon EKS-Add-On-Agenten der Version (`aws-guardduty-agent`) 1.5.0 und früher hosten. AWS-Region

AWS-Region	Amazon-ECR-Repository-URI
USA West (Oregon)	`039403964562.dkr.ecr.us-west-2.amazonaws.com`
Europa (Paris)	`113643092156.dkr.ecr.eu-west-3.amazonaws.com`
Asien-Pazifik (Mumbai)	`610108029387.dkr.ecr.ap-south-1.amazonaws.com`
Asien-Pazifik (Hyderabad)	`618745550137.dkr.ecr.ap-south-2.amazonaws.com`
Kanada (Zentral)	`001188825231.dkr.ecr.ca-central-1.amazonaws.com`
Naher Osten (VAE)	`601769779514.dkr.ecr.me-central-1.amazonaws.com`
Europe (London)	`109118265657.dkr.ecr.eu-west-2.amazonaws.com`
Europa (Irland)	`373421517865.dkr.ecr.us-west-1.amazonaws.com`
USA Ost (Nord-Virginia)	`031903291036.dkr.ecr.us-east-1.amazonaws.com`
USA Ost (Ohio)	`591382732059.dkr.ecr.us-east-2.amazonaws.com`

AWS-Region	Amazon-ECR-Repository-URI
Europa (Irland)	673884943994.dkr.ecr.eu-west-1.amazonaws.com
Südamerika (São Paulo)	941219317354.dkr.ecr.sa-east-1.amazonaws.com
Europa (Stockholm)	366771026645.dkr.ecr.eu-north-1.amazonaws.com
Europa (Frankfurt)	409493279830.dkr.ecr.eu-central-1.amazonaws.com
Europa (Zürich)	718440343717.dkr.ecr.eu-central-2.amazonaws.com
Asien-Pazifik (Singapur)	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
Asien-Pazifik (Sydney)	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
Asien-Pazifik (Jakarta)	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
Asien-Pazifik (Tokio)	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
Asien-Pazifik (Seoul)	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asien-Pazifik (Osaka)	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Asien-Pazifik (Hongkong)	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Naher Osten (Bahrain)	541829937850.dkr.ecr.me-south-1.amazonaws.com
Europa (Milan)	528450769569.dkr.ecr.eu-south-1.amazonaws.com

AWS-Region	Amazon-ECR-Repository-URI
Europa (Spain)	`531047660167.dkr.ecr.eu-south-2.amazonaws.com`
Afrika (Kapstadt)	`379032919888.dkr.ecr.af-south-1.amazonaws.com`
Asien-Pazifik (Melbourne)	`750462861327.dkr.ecr.ap-southeast-4.amazonaws.com`
Israel (Tel Aviv)	`292660727137.dkr.ecr.il-central-1.amazonaws.com`

Repository für GuardDuty Agenten auf AWS Fargate (nur Amazon ECS)

Die folgende Tabelle zeigt die Amazon ECR-Repositorys, die jeweils den GuardDuty Agenten für AWS Fargate (nur Amazon ECS) hosten. AWS-Region

AWS-Region	Amazon-ECR-Repository-URI
USA West (Oregon)	`733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Paris)	`665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Mumbai)	`251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Hyderabad)	`950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guardduty-agent-fargate`
Kanada (Zentral)	`354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Naher Osten (VAE)	`000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Europe (London)	`892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-fargate`

AWS-Region	Amazon-ECR-Repository-URI
Europa (Irland)	684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-fargate
USA Ost (Nord-Virginia)	593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-fargate
USA Ost (Ohio)	307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-fargate
Europa (Irland)	694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-fargate
Südamerika (São Paulo)	758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Stockholm)	591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Frankfurt)	323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Zürich)	529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-fargate
Asien-Pazifik (Singapur)	174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-fargate
Asien-Pazifik (Sydney)	005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-fargate
Asien-Pazifik (Jakarta)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asien-Pazifik (Tokio)	533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate
Asien-Pazifik (Seoul)	914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate

AWS-Region	Amazon-ECR-Repository-URI
Asien-Pazifik (Osaka)	`273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Hongkong)	`258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate`
Naher Osten (Bahrain)	`536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Milan)	`266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Spain)	`919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate`
Afrika (Kapstadt)	`197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Melbourne)	`251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate`
Israel (Tel Aviv)	`870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate`

GuardDuty Versionsverlauf des Agenten

Die folgenden Abschnitte enthalten die Release-Version für den GuardDuty Agenten, der auf Amazon EC2 EC2-Instances, Amazon ECS-Clustern und Amazon EKS-Clustern bereitgestellt wird

GuardDuty Sicherheitsagent für Amazon EC2 EC2-Instances

Agent-Version	Versionshinweise	Datum der Verfügbarkeit
v1.1.0	Unterstützt die GuardDuty automatische Agentenkonfiguration in Runtime	26. März 2024

Agent-Version	Versionshinweise	Datum der Verfügbarkeit
	Monitoring für Amazon EC2 EC2-Instances. Unterstützt neue Sicherhei tssignale und Erkenntnisse, die mit der Ankündigung der allgemeinen Verfügbarkeit von Runtime Monitoring für EC2-Instances veröffentlicht wurden. Allgemeine Leistungs verbesserung.	
v1.0.2	Unterstützt die neuesten Amazon ECS-AMIs.	2. Februar 2024
v1.0.1	Allgemeine Leistungsoptimieru ng und -verbesserungen Agentenversionen, die vor Version 1.0.2 veröffentlicht wurden, sind nicht mit Amazon ECS-AMIs kompatibel, die nach dem 31. Januar 2024 gestartet wurden.	23. Januar 2024
v1.0.0	Erste Version der RPM-Insta llation. Agentenversionen, die vor Version 1.0.2 veröffentlicht wurden, sind nicht mit Amazon ECS-AMIs kompatibel, die nach dem 31. Januar 2024 gestartet wurden.	26. November 2023

Der öffentliche Schlüssel, die Signatur von x86_64 RPM, die Signatur von arm64 RPM und der entsprechende Zugriffslink zu den RPM-Skripten, die in Amazon S3 S3-Buckets gehostet werden, können aus den folgenden Vorlagen gebildet werden. Ersetzen Sie den Wert von AWS-Region, der AWS Konto-ID und der GuardDuty Agentenversion, um auf die RPM-Skripts zuzugreifen. Die folgenden Vorlagen enthalten die neueste Agentenversion für Amazon EC2 EC2-Instances.

- Öffentlicher Schlüssel:

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/publickey.pem
```

- GuardDuty RPM-Signatur des Security Agents:

  Signatur von x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/amazon-guardduty-agent-1.1.0.x86_64.sig
```

  Signatur von arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/amazon-guardduty-agent-1.1.0.arm64.sig
```

- Greifen Sie auf Links zu den RPM-Skripten im Amazon S3 S3-Bucket zu:

  Zugangslink für x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/amazon-guardduty-agent-1.1.0.x86_64.rpm
```

  Zugangslink für arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/amazon-guardduty-agent-1.1.0.arm64.rpm
```

AWS-Region	Name der Region	AWS Konto-ID
eu-west-1	Europa (Irland)	694911143906
us-east-1	USA Ost (Nord-Virginia)	593207742271

us-east-2	USA Ost (Ohio)	733349766148
eu-west-3	Europa (Paris)	665651866788
us-east-2	USA Ost (Ohio)	307168627858
eu-central-1	Europa (Frankfurt)	323658145986
ap-northeast-2	Asien-Pazifik (Seoul)	914738172881
eu-north-1	Europa (Stockholm)	591436053604
ap-east-1	Asien-Pazifik (Hongkong)	258348409381
me-south-1	Naher Osten (Bahrain)	536382113932
eu-west-2	Europa (London)	892757235363
ap-northeast-1	Asien-Pazifik (Tokio)	533107202818
ap-southeast-1	Asien-Pazifik (Singapur)	174946120834
ap-south-1	Asien-Pazifik (Mumbai)	251508486986
ap-southeast-3	Asien-Pazifik (Jakarta)	510637619217
sa-east-1	Südamerika (São Paulo)	758426053663
ap-northeast-3	Asien-Pazifik (Osaka)	273192626886
eu-south-1	Europa (Milan)	266869475730
af-south-1	Afrika (Kapstadt)	197869348890
ap-southeast-2	Asien-Pazifik (Sydney)	005257825471
me-central-1	Naher Osten (VAE)	000014521398
us-west-1	USA West (Nordkalifornien)	684579721401
ca-central-1	Kanada (Zentral)	354763396469

ap-south-2	Asien-Pazifik (Hyderabad)	950823858135
eu-south-2	Europa (Spain)	919611009337
eu-central-2	Europa (Zürich)	529164026651
ap-southeast-4	Asien-Pazifik (Melbourne)	251357961535
il-central-1	Israel (Tel Aviv)	870907303882

GuardDuty Sicherheitsagent für AWS Fargate (nur Amazon ECS)

Die folgende Tabelle zeigt den Versionsverlauf für den GuardDuty Security Agent for Fargate (nur Amazon ECS).

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit
v1.2.0	x86_64 (AMD64): sha256:1dbad20ac2dc66d52d00bb28dde4281fe0d3c5f261b1649b247c2369d9e26b93 Graviton (ARM64): sha256:91930f8446f5f95b93b8ccb18773992affa401eb3f42da89d68077a56bafa6cd	Allgemeine Leistungsoptimierung und -verbesserungen	31. Mai 2024
v1.1.0	x86_64 (AMD64): sha256:83ce3cf2ef85a349ed1797a8cf30a008ac5d8c9f673f2835823957e9dcf71657 Graviton (ARM64): sha256:0d4b61648d7bdeab8ab8	Unterstützt neue Sicherheitssignale und Erkenntnisse Allgemeine Leistungs	01. Mai 2024

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit
	d94684f805498927c7d437d318204dcccfe8c9383dc7	optimierung und -verbesserungen	
v1.0.1	x86_64 (AMD64): sha256:9f8cd438fb66f62d09bfc641286439f7ed5177988a314a6021ef4ff880642e68 Graviton (ARM64): sha256:82c66bb615bd0d1e96db77b1f1fb51dc03220caa593b1962249571bf7147d1b7	Allgemeine Leistungsoptimierung und -verbesserungen	26. Januar 2024
v1.0.0	x86_64 (AMD64): sha256:359b8b014e5076c625daa1056090e522631587a7afa3b2e055edda6bd1141017 Graviton (ARM64): sha256:b9438690fa8a86067180a11658bec0f4f838ae3fbd225d04b9306250648b3984	Erste Version des GuardDuty Security Agents für AWS Fargate (nur Amazon ECS).	26. November 2023

GuardDuty Sicherheitsagent für Amazon EKS-Cluster

Die folgende Tabelle zeigt den Versionsverlauf des Amazon GuardDuty EKS-Add-On-Agenten.

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende des Standard-Supports [1]
v1.6.1	x86_64 (AMD64): `sha256:30650708a6601f6d6b9046f54b30f5fd65af296b1e40b8c24426b9bdb07c3ab1` Graviton (ARM64): `sha256:5f637c42ffb306b20f776d9d83e1e0b4be40ce245be44afcf43a8902b4d71019`	Allgemeine Leistungsoptimierung und -verbesserungen.	14. Mai 2024	–
v1.6.0	x86_64 (AMD64): `sha256:7dabcbee30d8b053676752fbc19e89f77272d9a6a53cc93731f5872180ef9010` Graviton (ARM64): `sha256:9710f53afccdf4f22b265a1a6fc27f1469403af1f7d5d08c4869a7269cdd2650`	• Unterstützt die GuardDuty automatische Agentenkonfiguration für EKS/EC2-Ressourcen. • Unterstützt die neuen Sicherheitssignale und Erkenntnisse. Weitere Informationen finden	29. April 2024	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende des Standard-Supports [1]
		Sie unter Gesammelte Runtime-Ereignistypen, die verwendet GuardDuty und Runtime Monitoring: Typen finden. • Allgemeine Leistungsoptimierung und -verbesserungen.		

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende des Standard-Supports [1]
v1.5.0	x86_64 (AMD64): `sha256:e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d` Graviton (ARM64): `sha256:afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6`	• Allgemeine Leistungsoptimierung und -verbesserungen. • Sicherheitsverbesserungen, einschließlich neuer Ereignistypen unterGesamme Laufzeit-Ereignistypen. • Leistungsverbesserungen rund um die CPU-Auslastung.	07. März 2024	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende des Standard-Supports [1]
v1.4.1	x86_64 (AMD64): `sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c` Graviton (ARM64): `sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dffe0792c9e6d0778b40`	Allgemeine Leistungsoptimierung und -verbesserungen.	16. Januar 2024	–
v1.4.0	x86_64 (AMD64): `sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f` Graviton (ARM64): `sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e`	Manifest-Mountpoints unterstützen eine bessere Datenerfassung AppArmor Konfiguration im Manifest Sammle das Befehlszeilenargument Allgemeine Leistungsoptimierung und -verbesserungen	21. Dezember 2	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende des Standard-Supports [1]
v1.3.1	x86_64 (AMD64): `sha256:55578fcb7b73097ade5c8404390ef16cf76a7b568490abaae01ac75992b3ea29` Graviton (ARM64): `sha256:e3ce8d66ac2121f8d476eb58f8bc50ab51336647615eb7cf514c21421cb818fd`	Wichtige Sicherheitspatches und Updates.	23. Oktober 202	–
v1.3.0	x86_64 (AMD64): `sha256:6dace2337dfbb7609811be89fb4b23ae0b865f1027ad78fbe69530bfbd46c694` Graviton (ARM64): `sha256:4928a7c6ef40e77c8ec95841323bb9a110db31f12c0ee7ab965e08b43efd01bb`	Unterstützt die Ubuntu-Plattform Unterstützt Kubernetes-Version 1.28 Allgemeine Leistungsverbesserungen und Stabilitätsverbesserungen.	5. Oktober 2023	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende des Standard-Supports [1]
v1.2.0	x86_64 (AMD64): `sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3` Graviton (ARM64): `sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa`	Zusätzlich zu AMD64-basierten Instances unterstützt v1.2.0 jetzt auch ARM64-basierte Instances . Unterstützung für Bottlerocket hinzugefügt und verifiziert Unterstützt Kubernetes-Version 1.27 Allgemeine Leistungsverbesserungen und Stabilitätsverbesserungen.	16. Juni 2023	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende des Standard-Supports [1]
v1.1.0	`sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c`	Über Kubernetes-Versionen, die vom Security Agent unterstützt werden GuardDuty hinaus unterstützt diese Agentenversion auch Kubernetes Version 1.26. Allgemeine Leistungsverbesserungen und Stabilitätsverbesserungen.	2. Mai 2023	14. Mai 2024
v1.0.0	`sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e`	Erste Version des Amazon-EKS-Add-On-Agenten.	30. März 2023	14. Mai 2024

- [1] Informationen zur Aktualisierung Ihrer aktuellen Agentenversion, für die der Standardsupport bald ausläuft, finden Sie unterManuelles Aktualisieren des Security Agents.

Auswirkungen der Deaktivierung und Bereinigung von Ressourcen

Dieser Abschnitt bezieht sich darauf, AWS-Konto ob Sie Runtime Monitoring oder nur die GuardDuty automatische Agentenkonfiguration für einen Ressourcentyp deaktivieren möchten.

GuardDuty Automatische Agentenkonfiguration deaktivieren

GuardDuty entfernt den Security Agent, der auf Ihrer Ressource installiert ist, nicht. GuardDuty Beendet jedoch die Verwaltung der Updates für den Security Agent.

GuardDuty empfängt weiterhin die Runtime-Ereignisse von Ihrem Ressourcentyp. Um Auswirkungen auf Ihre Nutzungsstatistiken zu vermeiden, sollten Sie den GuardDuty Security Agent unbedingt von Ihrer Ressource entfernen.

Unabhängig davon, ob ein gemeinsam genutzter VPC-Endpunkt AWS-Konto verwendet oder GuardDuty nicht, wird der VPC-Endpunkt nicht gelöscht. Falls erforderlich, müssen Sie den VPC-Endpunkt manuell löschen.

Runtime Monitoring und EKS Runtime Monitoring deaktivieren

Dieser Abschnitt gilt für Sie in den folgenden Szenarien:

- Sie haben EKS Runtime Monitoring nie separat aktiviert und jetzt haben Sie Runtime Monitoring deaktiviert.
- Sie deaktivieren sowohl Runtime Monitoring als auch EKS Runtime Monitoring. Wenn Sie sich über den Konfigurationsstatus von EKS Runtime Monitoring nicht sicher sind, finden Sie weitere Informationen unterÜberprüfen Sie den Konfigurationsstatus von EKS Runtime Monitoring.

Wenn die zuvor aufgelisteten Szenarien auf Sie zutreffen, GuardDuty wird in Ihrem Konto die folgenden Maßnahmen ergriffen:

- GuardDuty löscht die VPC mit dem Tag`GuardDutyManaged:true`. Dies ist die VPC, die für die Verwaltung des automatisierten Security Agents erstellt GuardDuty wurde.
- GuardDuty löscht die Sicherheitsgruppe, die als `GuardDutyManaged` gekennzeichnet wurde:. `true`
- Bei einer gemeinsam genutzten VPC, die von mindestens einem Teilnehmerkonto verwendet wurde, werden GuardDuty weder der VPC-Endpunkt noch die Sicherheitsgruppe gelöscht, die der gemeinsam genutzten VPC-Ressource zugeordnet ist.
- GuardDuty Löscht für eine Amazon EKS-Ressource den Security Agent. Dies ist unabhängig davon, ob die Verwaltung manuell oder über erfolgt GuardDuty.

Bei einer Amazon ECS-Ressource GuardDuty kann der Security Agent nicht von dieser Ressource deinstalliert werden, da eine ECS-Aufgabe unveränderlich ist. Dies ist unabhängig davon, wie Sie den Security Agent verwalten — manuell oder automatisch über GuardDuty. Nachdem Sie Runtime Monitoring deaktiviert haben, GuardDuty wird kein Sidecar-Container angehängt, wenn eine neue ECS-Task ausgeführt wird. Hinweise zur Arbeit mit Fargate-ECS-Aufgaben finden Sie unter. So funktioniert Runtime Monitoring mit Fargate (nur Amazon ECS)

GuardDuty Deinstalliert für eine Amazon EC2 EC2-Ressource den Security Agent nur dann von allen Systems Manager (SSM) verwalteten Amazon EC2 EC2-Instances, wenn er die folgenden Bedingungen erfüllt:

- Ihre Ressource ist nicht mit **`GuardDutyManaged`** dem Tag: Exclusion-Tag gekennzeichnet. `false`
- GuardDuty muss über Berechtigungen für den Zugriff auf die Tags in den Instanzmetadaten verfügen. Für diese EC2-Ressource ist der Zugriff auf Tags in Instanz-Metadaten auf Zulassen gesetzt.

Wenn Sie die manuelle Verwaltung des Security Agents beenden

Unabhängig davon, welche Methode Sie für die Installation und Verwaltung des GuardDuty Security Agents verwenden, müssen Sie den Security Agent entfernen, um die Überwachung der GuardDuty Runtime-Ereignisse in Ihrer Ressource zu beenden. Wenn Sie die Überwachung der Laufzeitereignisse von einem Ressourcentyp in einem Konto beenden möchten, können Sie auch den Amazon VPC-Endpunkt löschen.

Prozess zur Bereinigung der Ressourcen des Security Agents

So löschen Sie den Amazon VPC-Endpunkt

- Ohne gemeinsam genutzte VPC — Wenn Sie eine Ressource in einem Konto nicht mehr überwachen möchten, sollten Sie erwägen, den Amazon VPC-Endpunkt zu löschen.
- Mit einer gemeinsam genutzten VPC — Wenn ein gemeinsam genutztes VPC-Besitzerkonto die gemeinsam genutzte VPC-Ressource löscht, die noch verwendet wurde, kann der Deckungsstatus von Runtime Monitoring (und gegebenenfalls EKS Runtime Monitoring) für die Ressourcen in Ihrem gemeinsamen VPC-Eigentümerkonto und dem teilnehmenden Konto fehlerhaft werden. Informationen zum Deckungsstatus finden Sie unter. Bewertung der Laufzeitabdeckung Ihrer Ressourcen

Weitere Informationen finden Sie unter Löschen eines Schnittstellenendpunkts.

Um die Sicherheitsgruppe zu löschen

- Ohne gemeinsam genutzte VPC — Wenn Sie einen Ressourcentyp in einem Konto nicht mehr überwachen möchten, sollten Sie erwägen, die mit der Amazon VPC verknüpfte Sicherheitsgruppe zu löschen.
- Mit einer gemeinsam genutzten VPC — Wenn das gemeinsame VPC-Besitzerkonto die Sicherheitsgruppe löscht, kann es sein, dass jedes Teilnehmerkonto, das derzeit die mit der gemeinsam genutzten VPC verknüpfte Sicherheitsgruppe verwendet, der Runtime Monitoring-Abdeckungsstatus für die Ressourcen in Ihrem gemeinsamen VPC-Besitzerkonto und das teilnehmende Konto fehlerhaft werden. Weitere Informationen finden Sie unter Bewertung der Laufzeitabdeckung Ihrer Ressourcen.

Weitere Informationen finden Sie unter Löschen einer Sicherheitsgruppe.

Um den GuardDuty Security Agent aus einem EKS-Cluster zu entfernen

Informationen zum Entfernen des Security Agents aus Ihrem EKS-Cluster, den Sie nicht mehr überwachen möchten, finden Sie unter Löschen eines Add-ons.

Durch das Entfernen des EKS-Add-On-Agenten wird der `amazon-guardduty`-Namespace nicht aus dem EKS-Cluster entfernt. Um einen `amazon-guardduty`-Namespace zu löschen, sehen Sie Einen Namespace löschen.

So löschen Sie den **`amazon-guardduty`** Namespace (EKS-Cluster)

Wenn Sie die automatische Agentenkonfiguration deaktivieren, wird der `amazon-guardduty` Namespace nicht automatisch aus Ihrem EKS-Cluster entfernt. Um einen `amazon-guardduty`-Namespace zu löschen, sehen Sie Einen Namespace löschen.

Amazon S3 S3-Schutz bei Amazon GuardDuty

S3 Protection unterstützt Amazon bei der GuardDuty Überwachung von AWS CloudTrail Datenereignissen für Amazon Simple Storage Service (Amazon S3), die API-Operationen auf Objektebene beinhalten, um potenzielle Sicherheitsrisiken für Daten in Ihren Amazon S3-Buckets zu identifizieren.

GuardDuty überwacht sowohl AWS CloudTrail Verwaltungsereignisse als auch AWS CloudTrail S3-Datenereignisse, um potenzielle Bedrohungen in Ihren Amazon S3 S3-Ressourcen zu identifizieren. Beide Datenquellen überwachen verschiedene Arten von Aktivitäten. Beispiele für CloudTrail Verwaltungsereignisse für S3 sind Operationen, die Amazon S3 S3-Buckets auflisten oder konfigurieren, wie `ListBucketsDeleteBuckets`, und`PutBucketReplication`. Zu den Beispielen für CloudTrail Datenereignisse für S3 gehören API-Operationen auf Objektebene wie, `GetObjectListObjects`, `DeleteObject` und. `PutObject`

Wenn Sie Amazon GuardDuty für eine aktivieren AWS-Konto, GuardDuty beginnt die Überwachung von CloudTrail Verwaltungsereignissen. Sie müssen die Anmeldung bei S3-Datenereignissen nicht manuell aktivieren oder konfigurieren AWS CloudTrail. Sie können die S3-Schutzfunktion (die CloudTrail Datenereignisse für S3 überwacht) für jedes Konto an jedem AWS-Region Ort aktivieren, an dem diese Funktion bei Amazon verfügbar ist GuardDuty, jederzeit. Wer AWS-Konto bereits aktiviert ist GuardDuty, kann S3 Protection mit einer 30-tägigen kostenlosen Testphase zum ersten Mal aktivieren. Für Geräte AWS-Konto , die GuardDuty zum ersten Mal aktiviert werden, ist S3 Protection bereits aktiviert und in dieser kostenlosen 30-Tage-Testversion enthalten. Weitere Informationen finden Sie unter Schätzung der Kosten GuardDuty .

Wir empfehlen Ihnen, S3 Protection in GuardDuty zu aktivieren. Wenn diese Funktion nicht aktiviert ist, GuardDuty können Sie Ihre Amazon S3 S3-Buckets nicht vollständig überwachen oder Ergebnisse für verdächtigen Zugriff auf die in Ihren S3-Buckets gespeicherten Daten generieren.

Wie GuardDuty verwendet S3-Datenereignisse

Wenn Sie S3-Datenereignisse (S3 Protection) aktivieren, GuardDuty beginnt es mit der Analyse von S3-Datenereignissen aus all Ihren S3-Buckets und überwacht sie auf böswillige und verdächtige Aktivitäten. Weitere Informationen finden Sie unter AWS CloudTrail Datenereignisse für S3.

Wenn ein nicht authentifizierter Benutzer auf ein S3-Objekt zugreift, bedeutet dies, dass das S3-Objekt öffentlich zugänglich ist. Verarbeitet solche Anfragen daher GuardDuty nicht. GuardDuty

verarbeitet die an die S3-Objekte gestellten Anfragen unter Verwendung gültiger IAM (AWS Identity and Access Management) - oder AWS STS (AWS Security Token Service) -Anmeldeinformationen.

Wenn auf der Grundlage der Überwachung von S3-Datenereignissen eine potenzielle Bedrohung GuardDuty erkannt wird, wird eine Sicherheitsfeststellung generiert. Informationen zu den Arten von Ergebnissen, die für Amazon S3 S3-Buckets generiert werden GuardDuty können, finden Sie unterGuardDuty S3-Suchttypen.

Wenn Sie den S3-Schutz deaktivieren, wird die S3-Datenereignisüberwachung der in Ihren S3-Buckets gespeicherten Daten GuardDuty beendet.

S3 Protection für ein einzelnes Konto konfigurieren

Bei Konten, die mit verknüpft sind AWS Organizations, kann dieser Vorgang über die Konsoleneinstellungen automatisiert werden. Weitere Informationen finden Sie unter Konfigurieren von S3 Protection in Umgebungen mit mehreren Konten.

So aktivieren oder deaktivieren Sie S3 Protection

Wählen Sie Ihre bevorzugte Zugriffsmethode, um S3 Protection für ein einzelnes Konto zu konfigurieren.

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich S3 Protection.
3. Auf der Seite S3 Protection finden Sie den aktuellen Status von S3 Protection für Ihr Konto. Wählen Sie Aktivieren oder Deaktivieren, um S3 Protection zu einem beliebigen Zeitpunkt zu aktivieren oder zu deaktivieren.
4. Wählen Sie Bestätigen, um Ihre Auswahl zu bestätigen.

API/CLI

1. Führen Sie updateDetector unter Verwendung Ihrer gültige Detektor-ID für die aktuelle Region aus und übergeben Sie das `features`-Objekt `name` als `S3_DATA_EVENTS` auf `ENABLED` oder `DISABLED` gesetzt, um S3 Protection zu aktivieren oder zu deaktivieren.

> **Note**
>
> Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/ -Konsole.

2. Alternativ können Sie verwenden AWS Command Line Interface. Um S3 Protection zu aktivieren, führen Sie den folgenden Befehl aus und stellen Sie sicher, dass Sie Ihre eigene gültige Detektor-ID verwenden.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

Um S3 Protection zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED` im Beispiel.

Konfigurieren von S3 Protection in Umgebungen mit mehreren Konten

In einer Umgebung mit mehreren Konten hat nur das delegierte GuardDuty Administratorkonto die Möglichkeit, den S3-Schutz für die Mitgliedskonten in seiner AWS Organisation zu konfigurieren (zu aktivieren oder zu deaktivieren). Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Das delegierte GuardDuty Administratorkonto kann wählen, ob S3 Protection automatisch für alle Konten, nur für neue Konten oder für keine Konten in der Organisation aktiviert werden soll. Weitere Informationen finden Sie unter Verwalten von Konten mit AWS Organizations.

Konfiguration von S3 Protection für das delegierte Administratorkonto GuardDuty

Wählen Sie Ihre bevorzugte Zugriffsmethode, um S3 Protection für das delegierte GuardDuty Administratorkonto zu konfigurieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen des Verwaltungskontos verwenden.

2. Wählen Sie im Navigationsbereich S3 Protection.
3. Wählen Sie auf der Seite S3 Protection die Option Bearbeiten.
4. Führen Sie eine der folgenden Aktionen aus:

   Verwendung von Für alle Konten aktivieren

   - Wählen Sie Für alle Konten aktivieren. Dadurch wird der Schutzplan für alle aktiven GuardDuty Konten in Ihrer AWS Organisation aktiviert, einschließlich der neuen Konten, die der Organisation beitreten.
   - Wählen Sie Speichern.

   Verwendung von Konten manuell konfigurieren

   - Um den Schutzplan nur für das delegierte GuardDuty Administratorkonto zu aktivieren, wählen Sie Konten manuell konfigurieren.
   - Wählen Sie im Abschnitt für das delegierte GuardDuty Administratorkonto (dieses Konto) die Option Aktivieren aus.
   - Wählen Sie Speichern.

API/CLI

Verwenden Sie für die Ausführung updateDetectordie Detektor-ID des delegierten GuardDuty Administratorkontos für die aktuelle Region und übergeben Sie das `features` Objekt `name` als `S3_DATA_EVENTS` und `status` als `ENABLED` oder. `DISABLED`

Alternativ können Sie S3 Protection konfigurieren, indem Sie AWS Command Line Interface*Führen Sie den folgenden Befehl aus und achten Sie darauf, 12abc34d567e8fa901bc2d34e56789f0 durch die Detektor-ID des delegierten Administratorkontos für die aktuelle Region und 555555555555 durch die ID des delegierten Administratorkontos zu ersetzen. GuardDuty* AWS-Konto GuardDuty

Informationen zu den Einstellungen für Ihr Konto und Ihre aktuelle Region finden **`detectorId`** Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 555555555555 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

Automatisches Aktivieren von S3 Protection für alle Mitgliedskonten in der Organisation

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit Ihrem Administratorkonto an.

2. Führen Sie eine der folgenden Aktionen aus:

   Verwenden der Seite S3 Protection

   1. Wählen Sie im Navigationsbereich S3 Protection.
   2. Wählen Sie Für alle Konten aktivieren. Diese Aktion aktiviert automatisch S3 Protection sowohl für bestehende als auch für neue Konten in der Organisation.
   3. Wählen Sie Speichern.

      > **Note**
      >
      > Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

   Verwenden der Seite Konten

   1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
   2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren und anschließend Konten auf Einladung hinzufügen.
   3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten die Option Für alle Konten aktivieren unter S3 Protection.
   4. Wählen Sie Speichern.

Falls Sie die Option Für alle Konten aktivieren nicht verwenden können, finden Sie weitere Informationen unter Selektive Aktivierung oder Deaktivierung von S3 Protection in Mitgliedskonten.

API/CLI

- Um S3 Protection selektiv für Ihre neuen Konten zu aktivieren, rufen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen *`Detektor-ID`* auf.
- Das folgende Beispiel zeigt, wie Sie S3 Protection für ein einzelnes Mitgliedskonto aktivieren können. *`Achten Sie darauf, 12abc34d567e8fa901bc2d34e56789f0 durch das des delegierten Administratorkontos und 111122223333 zu ersetzen. detector-id GuardDuty`* Um S3 Protection zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Informationen zu `detectorId` den Einstellungen für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

  > **Note**
  >
  > Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivieren Sie S3 Protection für alle vorhandenen aktiven Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um S3 Protection für alle vorhandenen aktiven Mitgliedskonten in Ihrer Organisation zu aktivieren.

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldeinformationen für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich S3 Protection.
3. Auf der Seite S3 Protection können Sie den aktuellen Status der Konfiguration anzeigen. Wählen Sie im Abschnitt Aktive Mitgliedskonten die Option Aktionen.
4. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
5. Wählen Sie Bestätigen aus.

API/CLI

- Um S3 Protection selektiv für Ihre neuen Konten zu aktivieren, rufen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen *Detektor-ID* auf.
- Das folgende Beispiel zeigt, wie Sie S3 Protection für ein einzelnes Mitgliedskonto aktivieren können. *Achten Sie darauf, 12abc34d567e8fa901bc2d34e56789f0 durch das des delegierten Administratorkontos und 111122223333 zu ersetzen. detector-id GuardDuty* Um S3 Protection zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Informationen zu `detectorId` den Einstellungen für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Automatisches Aktivieren von S3 Protection für neue Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um S3 Protection für neue Konten, die Ihrer Organisation beitreten, zu aktivieren.

Console

Das delegierte GuardDuty Administratorkonto kann über die Konsole entweder über die Seite S3-Schutz oder Konten neue Mitgliedskonten in einer Organisation aktivieren.

So richten Sie Automatisches Aktivieren von S3 Protection für neue Mitgliedskonten ein

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Führen Sie eine der folgenden Aktionen aus:
   - Verwendung der Seite S3 Protection:
     1. Wählen Sie im Navigationsbereich S3 Protection.
     2. Wählen Sie auf der Seite S3 Protection die Option Bearbeiten.
     3. Wählen Sie Konten manuell konfigurieren.
     4. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Dieser Schritt stellt sicher, dass S3 Protection jedes mal automatisch für das Konto aktiviert wird, wenn ein neues Konto Ihrer Organisation beitritt. Nur das delegierte GuardDuty Administratorkonto der Organisation kann diese Konfiguration ändern.
     5. Wählen Sie Speichern.
   - Verwenden der Seite Konten:
     1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
     2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren.

3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter S3 Protection die Option Für neue Konten aktivieren.
4. Wählen Sie Speichern.

API/CLI

- Um S3 Protection selektiv für Ihre neuen Konten zu aktivieren, rufen Sie den API-Vorgang UpdateOrganizationConfiguration mit Ihrer eigenen *Detektor-ID* auf.
- Das folgende Beispiel zeigt, wie Sie S3 Protection für ein einzelnes Mitgliedskonto aktivieren können. Informationen zur Deaktivierung finden Sie unter Selektives Aktivieren oder Deaktivieren von RDS Protection für Mitgliedskonten. Legen Sie die Einstellungen so fest, dass der Schutzplan in dieser Region für neue Konten (`NEW`), die der Organisation beitreten, für alle Konten (`ALL`) oder für keines der Konten (`NONE`) in der Organisation automatisch aktiviert oder deaktiviert wird. Weitere Informationen finden Sie unter autoEnableOrganizationMitglieder. Je nach Ihren Einstellungen müssen Sie möglicherweise `NEW` durch `ALL` oder `NONE` ersetzen.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
   "S3_DATA_EVENTS", "autoEnable": "NEW"}]'
  ```

  > **Note**
  >
  > Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Selektive Aktivierung oder Deaktivierung von S3 Protection in Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um S3 Protection für bestimmte Mitgliedskonten zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.

   Auf der Seite Konten finden Sie in der Spalte S3 Protection den Status Ihres Mitgliedskontos.
3. So können Sie S3 Protection selektiv aktivieren und deaktivieren

   Wählen Sie das Konto aus, für das Sie S3 Protection konfigurieren möchten. Sie können mehrere Konten gleichzeitig auswählen. Wählen Sie im Dropdown-Menü Schutzpläne bearbeiten die Option S3Pro aus und wählen Sie dann die entsprechende Option aus.

API/CLI

Um S3 Protection selektiv für Ihre Mitgliedskonten zu aktivieren, rufen Sie den API-Vorgang updateMemberDetectors mit Ihrer eigenen Detektor-ID auf. Das folgende Beispiel zeigt, wie Sie S3 Protection für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `true` durch `false`.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
 aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012 --features
 '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

> **Note**
>
> Sie können auch eine Liste von Konto-IDs übergeben, die durch ein Leerzeichen getrennt sind.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

> **Note**
>
> Wenn Sie Skripts verwenden, um neue Konten zu integrieren und S3 Protection in Ihren neuen Konten deaktivieren möchten, können Sie den API-Vorgang createDetectormit dem optionalen `dataSources`-Objekt ändern, wie in diesem Thema beschrieben.

Automatisches Deaktivieren von S3 Protection für neue Konten GuardDuty

> **Important**
>
> Standardmäßig ist S3 Protection für AWS-Konten diesen Beitritt GuardDuty zum ersten Mal automatisch aktiviert.

Wenn Sie ein GuardDuty Administratorkonto haben, das GuardDuty zum ersten Mal für ein neues Konto aktiviert wird und Sie nicht möchten, dass S3 Protection standardmäßig aktiviert ist, können Sie es deaktivieren, indem Sie den createDetectorAPI-Vorgang mit dem optionalen `features` Objekt ändern. Im folgenden Beispiel wird der verwendet AWS CLI , um einen neuen GuardDuty Detektor bei deaktiviertem S3-Schutz zu aktivieren.

```
aws guardduty create-detector --enable --features '[{"Name" : "S3_DATA_EVENTS",
"Status" : "DISABLED"}]'
```

Feature in S3 Protection

AWS CloudTrail Datenereignisse für S3

Datenereignisse, auch bekannt als Vorgänge auf der Datenebene, bieten Einblicke in die Ressourcen-Vorgänge, die für oder innerhalb einer Ressource ausgeführt wurden. Datenereignisse sind oft Aktivitäten mit hohem Volume.

Im Folgenden finden Sie Beispiele für CloudTrail Datenereignisse für S3, die überwacht GuardDuty werden können:

- `GetObject`-API-Operationen
- `PutObject`-API-Operationen
- `ListObjects`-API-Operationen

- `DeleteObject`-API-Operationen

GuardDuty Bei der ersten Aktivierung ist S3 Protection standardmäßig aktiviert und auch in der 30-tägigen kostenlosen Testphase enthalten. Dieses Feature ist jedoch optional und Sie können sie jederzeit für jedes Konto oder jede Region aktivieren oder deaktivieren. Weitere Informationen zur Konfiguration von Amazon S3 als Feature finden Sie unter GuardDuty S3-Schutz.

Die GuardDuty Ergebnisse von Amazon verstehen

Ein GuardDuty Ergebnis steht für ein potenzielles Sicherheitsproblem, das in Ihrem Netzwerk erkannt wurde. GuardDutygeneriert immer dann einen Befund, wenn unerwartete und potenziell bösartige Aktivitäten in Ihrer AWS Umgebung entdeckt werden.

Sie können Ihre GuardDuty Ergebnisse auf der Ergebnisseite in der GuardDuty Konsole oder mithilfe der API-Operationen AWS CLI oder anzeigen und verwalten. Einen Überblick über die Möglichkeiten zur Verwaltung von Erkenntnissen finden Sie unter Verwaltung der GuardDuty Amazon-Ergebnisse.

Themen:

Erkenntnisdetails

Erfahren Sie mehr über die in den GuardDuty Ergebnissen verfügbaren Datentypen.

Beispielergebnisse

Erfahren Sie, wie Sie Stichprobenergebnisse generieren, um sie zu testen oder besser zu verstehen GuardDuty.

GuardDuty-Erkenntnisformat

Machen Sie sich mit dem Format der GuardDuty Erkennungstypen und den verschiedenen Bedrohungszwecken vertraut, die von ihnen verfolgt werden GuardDuty.

Erkenntnistypen

Sehen Sie sich alle verfügbaren Ergebnisse nach Typ GuardDuty an und durchsuchen Sie sie. Jeder Erkenntnistypeintrag enthält eine Erläuterung der betreffenden Erkenntnis sowie Tipps und Vorschläge für die Behebung.

Erkenntnisdetails

In der GuardDuty Amazon-Konsole können Sie die Details zu den Ergebnissen im Abschnitt Zusammenfassung der Ergebnisse einsehen. Die Erkenntnisdetails variieren je nach Erkenntnistyp.

Hauptsächlich bestimmen zwei Details, welche Arten von Informationen für jede Erkenntnis verfügbar sind. Das erste ist der Ressourcentyp, der `Instance`, `AccessKey`, `S3Bucket`, `Kubernetes cluster`, `ECS cluster`, `Container`, `RDSDBInstance` oder `Lambda` sein kann. Das zweite

Detail, das die Suche nach Informationen bestimmt, ist die Ressourcenrolle. Die Ressourcenrolle kann `Target` für Zugriffsschlüssel sein, was bedeutet, dass die Ressource das Ziel verdächtiger Aktivitäten war. Bei Feststellungen vom Typ Instance kann die Rolle der Ressource auch `Actor` sein, was bedeutet, dass Ihre Ressource der Akteur war, der die verdächtige Aktivität durchgeführt hat. In diesem Thema werden einige der allgemein verfügbaren Erkenntnisdetails beschrieben.

Überblick über Erkenntnisse

Der Abschnitt Überblick enthält die grundlegendsten Merkmale, anhand derer die Erkenntnis identifiziert werden kann, einschließlich der folgenden Informationen:

- Konto-ID — Die ID des AWS Kontos, in dem die Aktivität stattfand, die GuardDuty zur Generierung dieses Ergebnisses geführt hat.
- Anzahl — Gibt an, wie oft GuardDuty eine Aktivität, die diesem Muster entspricht, mit dieser Ergebnis-ID aggregiert wurde.
- Erstellt am – Uhrzeit und Datum des Zeitpunkts, an dem diese Erkenntnis erstmals erstellt wurde. Wenn dieser Wert von Aktualisiert am abweicht, bedeutet dies, dass die Aktivität mehrfach stattgefunden hat und ein fortlaufendes Problem darstellt.

> **Note**
>
> Zeitstempel für Ergebnisse in der GuardDuty Konsole werden in Ihrer lokalen Zeitzone angezeigt, während JSON-Exporte und CLI-Ausgaben Zeitstempel in UTC anzeigen.

- Erkenntnis-ID – Eine eindeutige Erkenntnis-ID für diesen Erkenntnistyp und Parametersatz. Neue Vorkommen von Aktivitäten, die diesem Muster entsprechen, werden für dieselbe ID aggregiert.
- Erkenntnistyp – Eine formatierte Zeichenfolge, die den Typ der Aktivität darstellt, durch den die Erkenntnis ausgelöst wurde. Weitere Informationen finden Sie unter GuardDuty-Erkenntnisformat.
- Region — Die AWS Region, in der das Ergebnis generiert wurde. Weitere Informationen zu unterstützten Regionen finden Sie unter Regionen und Endpunkte
- Ressourcen-ID — Die ID der AWS Ressource, für die die Aktivität stattgefunden hat, die GuardDuty zur Generierung dieses Ergebnisses geführt hat.
- Scan-ID — Gilt für Ergebnisse, wenn der GuardDuty Malware-Schutz aktiviert ist. Dabei handelt es sich um eine Kennung des Malware-Scans, der auf den EBS-Volumes ausgeführt wird, die an die potenziell gefährdete EC2-Instance oder den Container-Workload angehängt sind. Weitere Informationen finden Sie unter Details zu Erkenntnissen von Malware Protection.

- Schweregrad – der einer Erkenntnis zugeordnete Schweregrad: Hoch, Mittel oder Niedrig. Weitere Informationen finden Sie unter GuardDuty Schweregrade der Ergebnisse.
- Aktualisiert am — Das letzte Mal, als dieses Ergebnis mit einer neuen Aktivität aktualisiert wurde, die dem Muster entspricht, das GuardDuty zur Generierung dieses Ergebnisses geführt hat.

Ressource

Die betroffene Ressource enthält Einzelheiten zu der AWS Ressource, auf die die auslösende Aktivität abzielte. Die verfügbaren Informationen variieren je nach Ressourcentyp und Aktionstyp.

Ressourcenrolle — Die Rolle der AWS Ressource, die den Befund ausgelöst hat. Dieser Wert kann TARGET oder ACTOR lauten und repräsentiert, ob Ihre Ressource das Ziel verdächtiger Aktivitäten bzw. der Akteur war, der die verdächtigen Aktivitäten ausgeführt hat.

Ressourcen-Typ – der Typ der betroffenen Ressource. Wenn mehrere Ressourcen betroffen waren, kann eine Erkenntnis mehrere Ressourcentypen umfassen. Die Ressourcentypen sind Instance AccessKey, S3Bucket, ECSCluster KubernetesCluster, Container, RDSDBInstance und Lambda. Je nach Ressourcentyp stehen unterschiedliche Erkenntnisdetails zur Verfügung. Wählen Sie eine Registerkarte mit Ressourcenoptionen aus, um mehr über die für diese Ressource verfügbaren Details zu erfahren.

Instance

Instance-Details:

> **Note**
>
> Einige Instance-Details fehlen möglicherweise, wenn die Instance bereits gestoppt wurde oder wenn der zugrunde liegende API-Aufruf bei einem regionsübergreifenden API-Aufruf von einer EC2-Instance in einer anderen Region stammte.

- Instanz-ID — Die ID der EC2-Instance, die an der Aktivität beteiligt war, die zur Generierung des Ergebnisses geführt hat. GuardDuty
- Instance-Typ – Der Typ der EC2-Instance, der an der Erkenntnis beteiligt ist.
- Startzeit – Das Datum und die Uhrzeit, zu der die Instance gestartet wurde.
- Outpost ARN — Der Amazon-Ressourcenname (ARN) von AWS Outposts. Gilt nur für AWS Outposts Instances. Weitere Informationen finden Sie unter Was ist AWS Outposts?

- Name der Sicherheitsgruppe – Der Name der Sicherheitsgruppe, die der beteiligten Instance angefügt ist.
- Sicherheitsgruppen-ID – Die ID der Sicherheitsgruppe, die der beteiligten Instance angefügt ist.
- Instance-Status – Der aktuelle Status der Ziel-Instance.
- Availability Zone – Die Availability Zone der AWS -Region, in der sich die betroffene Instance befindet.
- Image-ID – Die ID des Amazon Machine Image, das zum Erstellen der an der Aktivität beteiligten Instance verwendet wurde.
- Image-Beschreibung – Eine Beschreibung der ID des Amazon Machine Image, das zum Erstellen der Instance verwendet wurde, die an der Aktivität beteiligt war.
- Tags – Eine Liste der Tags, die dieser Ressource angefügt sind, die im Format `key:value` aufgeführt werden.

AccessKey

Details zu Zugriffsschlüsseln:

- Zugriffsschlüssel-ID — Die Zugriffsschlüssel-ID des Benutzers, der an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Prinzipal-ID — Die Prinzipal-ID des Benutzers, der an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Benutzertyp — Der Benutzertyp, der an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat. Weitere Informationen finden Sie unter CloudTrail - Element userIdentity.
- Benutzername — Der Name des Benutzers, der an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.

S3Bucket

Details zum Amazon-S3-Bucket:

- Name – Der Name des Buckets, der an der Erkenntnis beteiligt war.
- ARN – Der ARN des Buckets, der an der Erkenntnis beteiligt war.

- Eigentümer – Die kanonische Benutzer-ID des Benutzers, dem der Bucket gehört, der an der Erkenntnis beteiligt war. Weitere Informationen zu kanonischen Benutzer-IDs finden Sie unter AWS -Konto-Kennungen.
- Typ – Der Typ der Bucket-Erkenntnis. Mögliche Werte sind Ziel oder Quelle.
- Standardmäßige serverseitige Verschlüsselung – Verschlüsselungsdetails für den Bucket.
- Bucket-Tags – Eine Liste der Tags, die dieser Ressource zugeordnet sind und im Format `key:value` aufgeführt werden.
- Effektive Berechtigungen – Eine Auswertung aller effektiven Berechtigungen und Richtlinien für den Bucket, die angibt, ob der betreffende Bucket öffentlich verfügbar ist. Werte können Öffentlich oder Nicht öffentlich sein.

EKSCluster

Details zum Kubernetes-Cluster:

- Name – Name des Kubernetes-Clusters.
- ARN – Der ARN, der den Cluster identifiziert.
- Erstellt am – Uhrzeit und Datum des Zeitpunkts, an dem dieser Cluster erstmals erstellt wurde.

> **Note**
>
> Zeitstempel für Ergebnisse in der GuardDuty Konsole werden in Ihrer lokalen Zeitzone angezeigt, während JSON-Exporte und CLI-Ausgaben Zeitstempel in UTC anzeigen.

- VPC-ID – Die ID der VPC, die Ihrem Cluster zugeordnet ist.
- Status – Der aktuelle Status des Clusters.
- Tags – Die Metadaten, die Sie auf den Cluster anwenden, um die Kategorisierung und Organisation zu erleichtern. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert, aufgelistet im Format `key:value`. Sie können sowohl den Schlüssel als auch den Wert definieren.

  Cluster-Tags werden nicht auf andere Ressourcen verteilt, die dem Cluster zugeordnet sind.

Details zum Kubernetes-Workload:

- Typ – Der Typ des Kubernetes-Workloads, wie Pod, Bereitstellung und Job.

- Name – Der Name des Kubernetes-Workloads.
- Uid – Die eindeutige ID des Kubernetes-Workloads.
- Erstellt am – Uhrzeit und Datum des Zeitpunkts, an dem dieser Workload erstmals erstellt wurde.
- Labels – Die Schlüssel-Wert-Paare, die dem Kubernetes-Workload angefügt wurden.
- Container – Die Details des Containers, der als Teil des Kubernetes-Workloads ausgeführt wird.
- Namespace – Der Workload gehört zu diesem Kubernetes-Namespace.
- Volumes – Die vom Kubernetes-Workload verwendeten Volumes.
  - Hostpfad – Stellt eine bereits vorhandene Datei oder ein Verzeichnis auf dem Host-Computer dar, dem das Volume zugeordnet ist.
  - Name – Der Name des Volumes.
- Pod-Sicherheitskontext – Definiert die Einstellungen für Rechte und Zugriffskontrolle für alle Container in einem Pod.
- Host-Netzwerk – Auf `true` setzen, wenn die Pods im Kubernetes-Workload enthalten sind.

Kubernetes-Benutzerdetails:

- Gruppen – Kubernetes-RBAC (Role-Access Based Control)-Gruppen des Benutzers, der an der Aktivität beteiligt war, die die Erkenntnis generiert hat.
- ID – Eindeutige ID des Kubernetes-Benutzers.
- Benutzername – Name des Kubernetes-Benutzers, der an der Aktivität beteiligt war, die das Ergebnis generiert hat.
- Sitzungsname – Entität, die die IAM-Rolle mit Kubernetes-RBAC-Berechtigungen übernommen hat.

ECSCluster

ECS-Cluster-Details:

- ARN – Der ARN, der den Cluster identifiziert.
- Name – Der Name des Clusters.
- Status – Der aktuelle Status des Clusters.
- Anzahl der aktiven Services – Die Anzahl der Services, die in einem `ACTIVE`-Status auf dem Cluster ausgeführt werden. Sie können diese Dienste mit anzeigen ListServices

- Anzahl registrierter Container-Instances – Die Anzahl der Container-Instances, die im Cluster registriert sind. Dazu gehören Container-Instances sowohl im Status `ACTIVE` als auch im Status `DRAINING`.
- Anzahl der laufenden Aufgaben – Die Anzahl der Aufgaben im Cluster, die sich im `RUNNING`-Status befinden.
- Tags – Die Metadaten, die Sie auf den Cluster anwenden, um die Kategorisierung und Organisation zu erleichtern. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert, aufgelistet im Format `key:value`. Sie können sowohl den Schlüssel als auch den Wert definieren.
- Container – Die Details zu dem Container, der der Aufgabe zugeordnet ist:
  - Containername – Der Name des Containers.
  - Container-Image – Das Image des Containers.
- Aufgabendetails – Die Details einer Aufgabe in einem Cluster.
  - ARN – Der Amazon-Ressourcenname (ARN) der Aufgabe.
  - Definition-ARN – Der Amazon-Ressourcenname (ARN) der Aufgabendefinition, die die Aufgabe erstellt.
  - Version – Der Versionszähler für die Aufgabe.
  - Aufgabe erstellt am – Der Unix-Zeitstempel für den Erstellungszeitpunkt der Aufgabe.
  - Aufgabe gestartet am – Der Unix-Zeitstempel für den Startzeitpunkt der Aufgabe.
  - Aufgabe gestartet von – Das Tag, das beim Starten einer Aufgabe angegeben wurde.

Container

Details zum Container:

- Container-Laufzeit – Die Container-Laufzeit (wie z. B. `docker` oder `containerd`), die zum Ausführen des Containers verwendet wurde.
- ID – Die Container-Instance-ID oder die vollständigen ARN-Einträge für die Container-Instance.
- Name – Der Name des Containers.

  Falls verfügbar, zeigt dieses Feld den Wert des Labels `io.kubenetes.container.name` an.
- Image – Das Image der Container-Instance.
- Volume-Mounts – Liste der Volume-Mounts von Containern. Ein Container kann ein Volume unter seinem Dateisystem mounten.

- Sicherheitskontext – Der Sicherheitskontext des Containers definiert Einstellungen für Rechte und Zugriffskontrolle für einen Container.
- Prozessdetails – Beschreibt die Details des Prozesses, der mit der Erkenntnis verknüpft ist.

RDSDBInstance

Details zur RDSDBInstance:

> **Note**
>
> Diese Ressource ist in den Erkenntnissen von RDS Protection im Zusammenhang mit der Datenbank-Instance verfügbar.

- Datenbankinstanz-ID — Der Bezeichner, der der Datenbankinstanz zugeordnet ist, die an der GuardDuty Suche beteiligt war.
- Engine – Der Name der Datenbank-Engine der Datenbank-Instance, die an der Erkenntnis beteiligt war. Mögliche Werte sind Aurora MySQL-kompatibel oder Aurora PostgreSQL-kompatibel.
- Engine-Version — Die Version der Datenbank-Engine, die an der GuardDuty Entdeckung beteiligt war.
- Datenbank-Cluster-ID — Der Bezeichner des Datenbank-Clusters, der die Datenbank-Instance-ID enthält, die an der GuardDuty Suche beteiligt war.
- Datenbankinstanz-ARN — Der ARN, der die an der GuardDuty Suche beteiligte Datenbankinstanz identifiziert.

Lambda

Details zur Lambda-Funktion

- Funktionsname – Der Name der Lambda-Funktion, die an der Erkenntnis beteiligt ist.
- Funktionsversion – Die Version der Lambda-Funktion, die an der Erkenntnis beteiligt ist.
- Funktionsbeschreibung – Eine Beschreibung der Lambda-Funktion, die an der Erkenntnis beteiligt ist.
- Funktions-ARN – Der Amazon-Ressourcenname (ARN) der Lambda-Funktion, die an der Erkenntnis beteiligt ist.

- Revisions-ID – Die Revisions-ID der Lambda-Funktionsversion.
- Rolle – Die Ausführungsrolle der Lambda-Funktion, die an der Erkenntnis beteiligt ist.
- VPC-Konfiguration – Die Amazon-VPC-Konfiguration, einschließlich der VPC-ID, Sicherheitsgruppe und Subnetz-IDs, die Ihrer Lambda-Funktion zugeordnet sind.
- VPC-ID – Die ID der Amazon-VPC, die der Lambda-Funktion zugeordnet ist, die an der Erkenntnis beteiligt ist.
- Subnetz-IDs – Die IDs der Subnetze, die Ihrer Lambda-Funktion zugeordnet sind.
- Sicherheitsgruppe – Die Sicherheitsgruppe, die der betroffenen Lambda-Funktion angefügt ist. Dazu gehören der Name und die Gruppen-ID der Sicherheitsgruppe.
- Tags – Eine Liste der Tags, die dieser Ressource angefügt sind, die im Format `key:value` aufgeführt werden.

Benutzerdetails für die RDS-Datenbank (DB)

> **Note**
>
> Dieser Abschnitt bezieht sich auf Ergebnisse, wenn Sie die RDS-Schutzfunktion in aktivieren GuardDuty. Weitere Informationen finden Sie unter GuardDuty RDS-Schutz.

Das GuardDuty Ergebnis enthält die folgenden Benutzer- und Authentifizierungsdetails der potenziell gefährdeten Datenbank.

- Benutzer – Der Benutzername, der für den anomalen Anmeldeversuch verwendet wurde.
- Anwendung – Der Anwendungsname, der für den anomalen Anmeldeversuch verwendet wurde.
- Datenbank – Der Name der Datenbank-Instance, die an dem anomalen Anmeldeversuch beteiligt war.
- SSL – Die für das Netzwerk verwendete Version von Secure Socket Layer (SSL).
- Authentifizierungsmethode – Die Authentifizierungsmethode, die von dem Benutzer verwendet wurde, der an der Erkenntnis beteiligt war.

Einzelheiten zu den Ergebnissen von Runtime Monitoring

> **Note**
>
> Diese Details sind möglicherweise nur verfügbar, wenn eines der GuardDuty generiert wirdRuntime Monitoring: Typen finden.

Dieser Abschnitt enthält die Laufzeitdetails wie Prozessdetails und den erforderlichen Kontext. Prozessdetails beschreiben Informationen über den beobachteten Prozess und der Laufzeitkontext beschreibt alle zusätzlichen Informationen über die potenziell verdächtige Aktivität.

Details zum Prozess

- Name – Der Name des Prozesses.
- Ausführbarer Pfad – Absoluter Pfad der ausführbaren Zieldatei des Prozesses.
- Ausführbarer SHA-256 – Der `SHA256`-Hash der ausführbaren Datei des Prozesses.
- Namespace-PID – Die Prozess-ID des Prozesses in einem sekundären PID-Namespace, bei dem es sich nicht um den PID-Namespace auf Host-Ebene handelt. Bei Prozessen innerhalb eines Containers ist dies die Prozess-ID, die innerhalb des Containers beobachtet wird.
- Derzeitiges Arbeitsverzeichnis – Das aktuelle Arbeitsverzeichnis des Prozesses.
- Prozess-ID – Die ID, die dem Prozess vom Betriebssystem zugewiesen wurde.
- Startzeit – Die Uhrzeit, zu der der Prozess gestartet wurde. Dieses Feld hat das UTC-Datums-Zeichenfolgenformat (`2023-03-22T19:37:20.168Z`).
- UUID — Die eindeutige ID, die dem Prozess von zugewiesen wurde. GuardDuty
- Parent UUID – Die eindeutige ID des übergeordneten Prozesses. Diese ID wird dem übergeordneten Prozess von zugewiesen. GuardDuty
- Benutzername – Der Benutzername, der den Prozess ausgeführt hat.
- Benutzer-ID – Die Benutzer-ID des Benutzers, der den Prozess ausgeführt hat.
- Effektive Benutzer-ID – Die effektive Benutzer-ID des Prozesses zum Zeitpunkt des Ereignisses.
- Herkunft – Informationen über die Vorfahren des Prozesses.
  - Prozess-ID – Die ID, die dem Prozess vom Betriebssystem zugewiesen wurde.
  - UUID — Die eindeutige ID, die dem Prozess von zugewiesen wurde. GuardDuty

- Ausführbarer Pfad – Absoluter Pfad der ausführbaren Zieldatei des Prozesses.
- Effektive Benutzer-ID – Die effektive Benutzer-ID des Prozesses zum Zeitpunkt des Ereignisses.
- Parent UUID – Die eindeutige ID des übergeordneten Prozesses. Diese ID wird dem übergeordneten Prozess von zugewiesen. GuardDuty
- Startzeit – Die Uhrzeit, zu der der Prozess gestartet wurde.
- Namespace-PID – Die Prozess-ID des Prozesses in einem sekundären PID-Namespace, bei dem es sich nicht um den PID-Namespace auf Host-Ebene handelt. Bei Prozessen innerhalb eines Containers ist dies die Prozess-ID, die innerhalb des Containers beobachtet wird.
- Benutzer-ID – Die Benutzer-ID des Benutzers, der den Prozess ausgeführt hat.
- Name – Der Name des Prozesses.

Laufzeitkontext

Aus den folgenden Feldern kann eine generierte Erkenntnis nur die Felder enthalten, die für den Erkenntnistyp relevant sind.

- Mount-Quelle – Der Pfad auf dem Host, der vom Container bereitgestellt wird.
- Mount-Ziel – Der Pfad im Container, der dem Host-Verzeichnis zugeordnet ist.
- Dateisystem-Typ – Stellt den Typ des eingehängten Dateisystems dar.
- Flags – Stellt Optionen dar, die das Verhalten des Ereignisses steuern, das an dieser Erkenntnis beteiligt ist.
- Verändernder Prozess – Informationen über den Prozess, der zur Laufzeit eine Binärdatei, ein Skript oder eine Bibliothek in einem Container erstellt oder geändert hat.
- Geändert am – Der Zeitstempel, zu dem der Prozess zur Laufzeit eine Binärdatei, ein Skript oder eine Bibliothek in einem Container erstellt oder geändert hat. Dieses Feld hat das UTC-Datums-Zeichenfolgenformat (`2023-03-22T19:37:20.168Z`).
- Bibliothekspfad – Der Pfad zur neuen Bibliothek, die geladen wurde.
- LD-Vorladungs-Wert – Der Wert der `LD_PRELOAD`-Umgebungsvariable.
- Socket-Pfad – Der Pfad zum Docker-Socket, auf den zugegriffen wurde.
- Runc-Binär-Pfad – Der Pfad zur `runc`-Binärdatei.
- Release-Agent-Pfad – Der Pfad zur `cgroup`-Release-Agent-Datei.
- Beispiel für eine Befehlszeile — Das Beispiel der Befehlszeile, die an der potenziell verdächtigen Aktivität beteiligt war.

- Werkzeugkategorie — Kategorie, zu der das Tool gehört. Einige der Beispiele sind Backdoor Tool, Pentest Tool, Network Scanner und Network Sniffer.
- Toolname — Der Name des potenziell gefährlichen Tools.
- Skriptpfad — Der Pfad zu dem ausgeführten Skript, das den Befund generiert hat.
- Pfad der Bedrohungsdatei — Der verdächtige Pfad, für den die Bedrohungsinformationen gefunden wurden.
- Dienstname — Der Name des Sicherheitsdienstes, der deaktiviert wurde.

Scan-Details der EBS-Volumes

> **Note**
>
> Dieser Abschnitt bezieht sich auf Ergebnisse, die beim Einschalten des GuardDuty -initiierten Malware-Scans in GuardDuty Schutz vor Schadsoftware festgestellt wurden.

Der EBS-Volume-Scan liefert Details über das EBS-Volume, das an die potenziell kompromittierte EC2-Instance oder den Container-Workload angehängt ist.

- Scan-ID – Die Kennung des Malware-Scans.
- Scan gestartet am – Das Datum und die Uhrzeit, zu der der Malware-Scan gestartet wurde.
- Scan abgeschlossen am – Das Datum und die Uhrzeit, zu der der Malware-Scan abgeschlossen wurde.
- Trigger Finding ID — Die Finde-ID des GuardDuty Fundes, das diesen Malware-Scan ausgelöst hat.
- Quellen – Die möglichen Werte sind `Bitdefender` und `AWS`.
- Scan-Erkennungen – Die vollständige Ansicht der Details und Ergebnisse jedes Malware-Scans.
  - Anzahl gescannter Objekte – Die Gesamtzahl der gescannten Dateien. Liefert Details wie `totalGb`, `files` und `volumes`.
  - Anzahl der entdeckten Bedrohungen – Die Gesamtzahl der während des Scans erkannten schädlichen `files`.
  - Bedrohungsdetails mit dem höchsten Schweregrad – Die Details der Bedrohung mit dem höchsten Schweregrad, die während des Scans erkannt wurde, und die Anzahl der schädlichen Dateien. Liefert Details wie `severity`, `threatName` und `count`.

- Nach Namen erkannte Bedrohungen – Das Container-Element, in dem Bedrohungen aller Schweregrade gruppiert werden. Liefert Details wie `itemCount`, `uniqueThreatNameCount`, `shortened` und `threatNames`.

Details zu Erkenntnissen von Malware Protection

> **Note**
>
> Dieser Abschnitt bezieht sich auf Ergebnisse, die sich ergeben, wenn Sie den GuardDuty -initiierten Malware-Scan in GuardDuty Schutz vor Schadsoftware einschalten.

Wenn beim Malware-Protection-Scan Malware erkannt wird, können Sie die Scandetails anzeigen, indem Sie auf der Seite Erkenntnisse in der https://console.aws.amazon.com/guardduty/-Konsole das entsprechende Ergebnis auswählen. Der Schweregrad Ihres Malware-Schutz-Ergebnisses hängt vom Schweregrad des GuardDuty Fehlers ab.

> **Note**
>
> Das `GuardDutyFindingDetected`-Tag gibt an, dass die Snapshots Malware enthalten.

Die folgenden Informationen sind im Abschnitt Entdeckte Bedrohungen im Detailbereich verfügbar.

- Name – Der Name der Bedrohung, der durch Gruppierung der Dateien nach Entdeckung ermittelt wurde.
- Schweregrad – Der Schweregrad der erkannten Bedrohung.
- Hash – Der SHA-256-Hashwert der Datei.
- Dateipfad – Der Speicherort der schädlichen Datei auf dem EBS-Volume.
- Dateiname – Der Name der Datei, in der die Bedrohung erkannt wurde.
- Volume-ARN – Der ARN der gescannten EBS-Volumes.

Die folgenden Informationen sind im Abschnitt Malware-Scan-Details im Detailbereich verfügbar.

- Scan-ID – Die Kennung des Malware-Scans.

- Scan gestartet am – Das Datum und die Uhrzeit, zu der der Malware-Scan gestartet wurde.
- Scan abgeschlossen am – Das Datum und die Uhrzeit, zu der der Scan abgeschlossen wurde.
- Gescannte Dateien – Die Gesamtzahl der gescannten Dateien und Verzeichnisse.
- Gescannte GB insgesamt – Die Menge an Speicherplatz, die während des Vorgangs gescannt wurde.
- Erkennungs-ID des Auslösers — Die Finde-ID des GuardDuty Fundes, das diesen Malware-Scan ausgelöst hat.
- Die folgenden Informationen sind im Abschnitt Volume-Details im Detailbereich verfügbar.
  - Volume-ARN – Der Amazon-Ressourcenname (ARN) des Volumes.
  - Snapshot-ARN – Der ARN des Snapshots des EBS-Volumes.
  - Status – Der Scan-Status des Volumes, z. B. `Running`, `Skipped` und `Completed`.
  - Verschlüsselungstyp – Der Verschlüsselungstyp, der zur Verschlüsselung des Volumes verwendet wird. z. B. `CMCMK`.
  - Gerätename – Der Name des Geräts. z. B. `/dev/xvda`.

Aktion

Die Aktion einer Erkenntnis gibt Details über die Art der Aktivität, durch die das Ergebnis ausgelöst wurde. Die verfügbaren Informationen variieren je nach Aktionstyp.

Aktionstyp – Der Aktivitätstyp der Erkenntnis. Dieser Wert kann NETWORK_CONNECTION, PORT_PROBE, DNS_REQUEST, AWS_API_CALL oder RDS_LOGIN_ATTEMPT sein. Die verfügbaren Informationen variieren je nach Aktionstyp:

- NETWORK_CONNECTION – Gibt an, dass Netzwerkdatenverkehr zwischen der identifizierten EC2-Instance und dem Remote-Host ausgetauscht wurde. Dieser Aktionstyp enthält die folgenden zusätzlichen Informationen:
  - Verbindungsrichtung — Die Netzwerkverbindungsrichtung, die bei der Aktivität beobachtet wurde, die GuardDuty zur Generierung des Ergebnisses geführt hat. Bei ihnen kann es sich um einen der folgenden Werte handeln:
    - INBOUND – Gibt an, dass ein Remote-Host eine Verbindung mit einem lokalen Port auf der in Ihrem Konto identifizierten EC2-Instance initiiert hat.
    - OUTBOUND – Gibt an, dass die identifizierte EC2-Instance eine Verbindung mit einem Remote-Host initiiert hat.

    - UNBEKANNT — Zeigt an, dass die Richtung der Verbindung nicht bestimmt werden GuardDuty konnte.
  - Protokoll — Das Netzwerkverbindungsprotokoll, das bei der Aktivität beobachtet wurde, die GuardDuty zur Generierung des Ergebnisses geführt hat.
  - Lokale IP – Die ursprüngliche Quell-IP-Adresse des Datenverkehrs, der die Erkenntnis ausgelöst hat. Diese Informationen können verwendet werden, um zwischen der IP-Adresse einer Zwischenebene, durch die Datenverkehr fließt, und der ursprünglichen Quell-IP-Adresse des Datenverkehrs , der die Suche ausgelöst hat, zu unterscheiden. Zum Beispiel die IP-Adresse eines EKS-Pods im Gegensatz zur IP-Adresse der Instance, auf der der EKS-Pod ausgeführt wird.
  - Blockiert – Gibt an, ob der Ziel-Port blockiert ist.
- PORT_PROBE – Gibt an, dass ein Remote-Host die identifizierte EC2-Instance auf mehreren offenen Ports untersucht hat. Dieser Aktionstyp enthält die folgenden zusätzlichen Informationen:
  - Lokale IP – Die ursprüngliche Quell-IP-Adresse des Datenverkehrs, der die Erkenntnis ausgelöst hat. Diese Informationen können verwendet werden, um zwischen der IP-Adresse einer Zwischenebene, durch die Datenverkehr fließt, und der ursprünglichen Quell-IP-Adresse des Datenverkehrs , der die Suche ausgelöst hat, zu unterscheiden. Zum Beispiel die IP-Adresse eines EKS-Pods im Gegensatz zur IP-Adresse der Instance, auf der der EKS-Pod ausgeführt wird.
  - Blockiert – Gibt an, ob der Ziel-Port blockiert ist.
- DNS_REQUEST – Gibt an, dass die identifizierte EC2-Instance einen Domainnamen abgefragt hat. Dieser Aktionstyp enthält die folgenden zusätzlichen Informationen:
  - Protokoll — Das Netzwerkverbindungsprotokoll, das bei der Aktivität beobachtet wurde, die GuardDuty zur Generierung des Ergebnisses führte.
  - Blockiert – Gibt an, ob der Ziel-Port blockiert ist.
- AWS_API_CALL – Gibt an, dass eine AWS -API aufgerufen wurde. Dieser Aktionstyp enthält die folgenden zusätzlichen Informationen:
  - API — Der Name des API-Vorgangs, der aufgerufen und somit GuardDuty zur Generierung dieses Ergebnisses aufgefordert wurde.

> **Note**
>
> Diese Vorgänge können auch Nicht-API-Ereignisse einschließen, die von AWS CloudTrail erfasst wurden. Weitere Informationen finden Sie unter Nicht-API-Ereignisse, die von erfasst wurden. CloudTrail

  - Benutzeragent – Der Benutzeragent, der die API-Anfrage gestellt hat. Dieser Wert gibt an, ob der Aufruf über den AWS Management Console, einen AWS Dienst, die AWS SDKs oder den erfolgte. AWS CLI
  - ERROR_CODE – Wenn die Erkenntnis durch einen fehlgeschlagenen API-Aufruf ausgelöst wurde, wird der Fehlercode für diesen Aufruf angezeigt.
  - Service-Name – Der DNS-Name des Services, der versucht hat, den API-Aufruf durchzuführen, durch den die Erkenntnis ausgelöst wurde.
- RDS_LOGIN_ATTEMPT – Zeigt an, dass von einer Remote-IP-Adresse aus ein Anmeldeversuch bei der potenziell kompromittierte Datenbank unternommen wurde.
  - IP-Adresse – Die Remote-IP-Adresse, die für den potenziell verdächtigen Anmeldeversuch verwendet wurde.

Akteur oder Ziel

Eine Erkenntnis verfügt über den Abschnitt Actor, wenn die Ressourcenrolle `TARGET` war. Dies zeigt an, dass verdächtige Aktivitäten auf Ihre Ressource ausgerichtet waren, und der Abschnitt Actor enthält Details zur Entität, von der diese auf Ihre Ressource ausgerichtet wurden.

Eine Erkenntnis hat einen Ziel-Abschnitt, wenn die Ressourcenrolle `ACTOR` lautete. Dies zeigt an, dass Ihre Ressource an verdächtigen Aktivitäten gegen einen Remote-Host beteiligt war. Dieser Abschnitt enthält Informationen zur IP-Adresse und/oder Domain, auf die Ihre Ressource ausgerichtet ist.

Im Abschnitt Actor oder Ziel können folgende Informationen verfügbar sein:

- Verbunden — Details darüber, ob das AWS Konto des Remote-API-Aufrufers mit Ihrer GuardDuty Umgebung verknüpft ist. Wenn dieser Wert `true` ist, ist der API-Aufrufer in irgendeiner Weise Ihrem Konto zugeordnet. Falls der Wert `false` ist, stammt der API-Aufrufer von außerhalb Ihrer Umgebung.

- Remote-Konto-ID — Die Konto-ID, der die ausgehende IP-Adresse gehört, die für den Zugriff auf die Ressource im endgültigen Netzwerk verwendet wurde.
- IP-Adresse — Die IP-Adresse, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Standort — Standortinformationen für die IP-Adresse, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Organisation — Informationen zur ISP-Organisation der IP-Adresse, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Port — Die Portnummer, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Domain — Die Domain, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Domain mit Suffix — Die Domain der zweiten und obersten Ebene, die an einer Aktivität beteiligt war, die möglicherweise GuardDuty zur Generierung des Ergebnisses geführt hat. Eine Liste der Domänen der obersten und zweiten Ebene finden Sie in der Liste der öffentlichen Suffixe.

Zusätzliche Informationen

Alle Erkenntnisse verfügen über einen Abschnitt Zusätzliche Informationen, der die folgenden Informationen enthalten kann:

- Name der Bedrohungsliste — Der Name der Bedrohungsliste, die die IP-Adresse oder den Domainnamen enthält, der an der Aktivität beteiligt war, die GuardDuty zur Generierung des Fundes geführt hat.
- Beispiel – Der Wert Wahr oder Falsch, gibt an, ob es sich um ein Beispiel-Erkenntnis handelt.
- Archiviert – Der Wert Wahr oder Falsch, gibt an, ob diese Erkenntnis archiviert wurde.
- Ungewöhnlich – Aktivitätsdetails, die zuvor noch nicht beobachtet wurden. Dabei kann es sich um ungewöhnliche (zuvor nicht beobachtete) Benutzer, Standorte, Zeitpunkte, Buckets, Anmeldeverhalten oder ASN Org handeln.
- Ungewöhnliches Protokoll — Das Netzwerkverbindungsprotokoll, das an der Aktivität beteiligt war, die GuardDuty zur Generierung des Befundes geführt hat.
- Agentendetails – Details über den Sicherheitsagent, der derzeit auf dem EKS-Cluster in Ihrem AWS-Konto installiert ist. Dies gilt nur für Erkenntnistypen von der EKS-Laufzeit-Überwachung.
  - Agent-Version — Die Version des GuardDuty Security Agents.

- Agenten-ID — Die eindeutige Kennung des GuardDuty Security Agents.

Beweise

Erkenntnisse, die auf Bedrohungsinformationen basieren, haben einen Abschnitt Beweise, der die folgenden Informationen enthält:

- Informationen zur Bedrohungsinformation — Der Name der Bedrohungsliste, auf der die erkannte Bedrohung aufgeführt `Threat name` ist.
- Name der Bedrohung — Der Name der Malware-Familie oder eine andere Kennung, die mit der Bedrohung verknüpft ist.
- Bedrohungsdatei SHA256 — SHA256 der Datei, die den Befund generiert hat.

Anormales Verhalten

Arten von Ergebnissen, die auf enden, AnomalousBehaviorweisen darauf hin, dass der Befund durch das ML-Modell (Machine Learning) zur Erkennung von GuardDuty Anomalien generiert wurde. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde.

Einzelheiten darüber, welche Faktoren der API-Anfrage für die CloudTrail Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Ergebnisdetails. Die Identitäten werden durch das CloudTrail UserIdentity-Element definiert, und die möglichen Werte sind:`Root`,,, `IAMUserAssumedRole`, `FederatedUser` oder. `AWSAccount` `AWSService`

Zusätzlich zu den Informationen, die für alle GuardDuty Ergebnisse im Zusammenhang mit API-Aktivitäten verfügbar sind, enthalten die AnomalousBehaviorErgebnisse zusätzliche Details, die im folgenden Abschnitt beschrieben werden. Diese Details können in der Konsole eingesehen werden und sind auch in der JSON-Datei des Erkenntnisses verfügbar.

- Anomale APIs – Eine Liste von API-Anfragen, die von der Benutzeridentität in der Nähe der mit der Erkenntnis verknüpften primären API-Anfrage aufgerufen wurden. In diesem Bereich werden die Details des API-Erkenntnisses wie folgt weiter aufgeschlüsselt.
  - Bei der ersten aufgeführten API handelt es sich um die primäre API, d. h. um die API-Anfrage, die mit der beobachteten Aktivität mit dem höchsten Risiko verknüpft ist. Dies ist die API, welche

die Erkenntnis ausgelöst hat und mit der Angriffsphase des Erkenntnistyps korreliert. Dies ist auch die API, die im Abschnitt Aktion in der Konsole und in der JSON-Datei des Erkenntnisses detailliert beschrieben wird.

- Bei allen anderen aufgeführten APIs handelt es sich um zusätzliche anomale APIs, die anhand der aufgelisteten Benutzeridentität in der Nähe der primären API beobachtet wurden. Wenn nur eine API auf der Liste steht, hat das ML-Modell keine zusätzlichen API-Anfragen von dieser Benutzeridentität als anomal identifiziert.
- Die Liste der APIs ist danach unterteilt, ob eine API erfolgreich aufgerufen wurde oder ob die API erfolglos aufgerufen wurde, was bedeutet, dass eine Fehlerantwort empfangen wurde. Die Art der empfangenen Fehlerantwort ist über jeder API aufgeführt, die erfolglos aufgerufen wurde. Mögliche Fehlerantworttypen sind: `access denied`, `access denied exception`, `auth failure`, `instance limit exceeded`, `invalid permission - duplicate`, `invalid permission - not found` und `operation not permitted`.
- APIs werden nach dem zugehörigen Service kategorisiert.

> **Note**
>
> Wenn Sie mehr Kontext benötigen, wählen Sie Historische APIs aus, um die Details zu den wichtigsten APIs (maximal 20) anzuzeigen, die normalerweise sowohl für die Benutzeridentität als auch für alle Benutzer innerhalb des Kontos angezeigt werden. Die APIs sind als Selten (weniger als einmal pro Monat), Gelegentlich (einige Male im Monat) oder Häufig (täglich bis wöchentlich) gekennzeichnet, je nachdem, wie oft sie in Ihrem Konto verwendet werden.

- Ungewöhnliches Verhalten (Konto) – In diesem Abschnitt finden Sie zusätzliche Informationen zum profilierten Verhalten Ihres Kontos. Zu den in diesem Bereich erfassten Informationen gehören:
  - ASN-Organisation – Die ASN-Organisation, von der aus der anomale API-Aufruf getätigt wurde.
  - Benutzername – Der Name des Benutzers, der den anomalen API-Aufruf ausgeführt hat.
  - Benutzeragent – Der Benutzeragent, der für den anomalen API-Aufruf verwendet wurde. Der Benutzeragent ist die Methode, mit der der Aufruf ausgeführt wird, z. B. `aws-cli` oder `Botocore`.
  - Benutzertyp – Der Typ des Benutzers, der den anomalen API-Aufruf ausgeführt hat. Mögliche Werte sind `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` oder `ROLE`.
  - Bucket – Der Name des S3-Buckets, auf den zugegriffen wurde.

- Ungewöhnliches Verhalten (Benutzeridentität) – Dieser Abschnitt enthält zusätzliche Informationen zum profilierten Verhalten der Benutzeridentität, die an der Erkenntnis beteiligt war. Wenn ein Verhalten nicht als historisch identifiziert wurde, bedeutet dies, dass das GuardDuty ML-Modell noch nie gesehen hat, dass diese Benutzeridentität diesen API-Aufruf innerhalb des Trainingszeitraums auf diese Weise ausgeführt hat. Die folgenden zusätzlichen Details zur Benutzeridentität sind verfügbar:
  - ASN Org – Die ASN-Organisation, von der aus der anomale API-Aufruf getätigt wurde.
  - Benutzeragent – Der Benutzeragent, der für den anomalen API-Aufruf verwendet wurde. Der Benutzeragent ist die Methode, mit der der Aufruf ausgeführt wird, z. B. `aws-cli` oder `Botocore`.
  - Bucket – Der Name des S3-Buckets, auf den zugegriffen wurde.
- Ungewöhnliches Verhalten (Bucket) – Dieser Abschnitt enthält zusätzliche Informationen zum profilierten Verhalten des S3-Buckets, der mit der Erkenntnis verknüpft ist. Wenn ein Verhalten nicht als historisch identifiziert wurde, bedeutet dies, dass das GuardDuty ML-Modell innerhalb des Trainingszeitraums noch keine API-Aufrufe auf diese Weise an diesen Bucket gesendet hat. Zu den in diesem Bereich erfassten Informationen gehören:
  - ASN Org – Die ASN-Organisation, von der aus der anomale API-Aufruf getätigt wurde.
  - Benutzername – Der Name des Benutzers, der den anomalen API-Aufruf ausgeführt hat.
  - Benutzeragent – Der Benutzeragent, der für den anomalen API-Aufruf verwendet wurde. Der Benutzeragent ist die Methode, mit der der Aufruf ausgeführt wird, z. B. `aws-cli` oder `Botocore`.
  - Benutzertyp – Der Typ des Benutzers, der den anomalen API-Aufruf ausgeführt hat. Mögliche Werte sind `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` oder `ROLE`.

  > **Note**
  >
  > Weitere Informationen zu historischen Verhaltensweisen finden Sie unter Historisches Verhalten in den Abschnitten Ungewöhnliches Verhalten (Konto), Benutzer-ID oder Bucket, wo Sie Details zum erwarteten Verhalten in Ihrem Konto für jede der folgenden Kategorien anzeigen können: Selten (weniger als einmal pro Monat), Gelegentlich (einige Male pro Monat) oder Häufig (täglich bis wöchentlich), je nachdem, wie oft sie in Ihrem Konto verwendet werden.
- Ungewöhnliches Verhalten (Datenbank) – Dieser Abschnitt enthält zusätzliche Informationen zum profilierten Verhalten der Datenbank-Instance, das mit der Erkenntnis verknüpft ist. Wenn

ein Verhalten nicht als historisch identifiziert wurde, bedeutet dies, dass das GuardDuty ML-Modell innerhalb des Trainingszeitraums noch keinen Anmeldeversuch auf diese Weise bei dieser Datenbankinstanz festgestellt hat. Zu den Informationen, die für diesen Abschnitt im Erkenntnisbereich verfolgt werden, gehören:

- Benutzer – Der Benutzername, der für den anomalen Anmeldeversuch verwendet wurde.
- ASN Org – Die ASN-Organisation, von der aus der anomale API-Aufruf getätigt wurde.
- Anwendung – Der Anwendungsname, der für den anomalen Anmeldeversuch verwendet wurde.
- Datenbank – Der Name der Datenbank-Instance, die an dem anomalen Anmeldeversuch beteiligt war.

> **Note**
>
> Der Abschnitt Historisches Verhalten bietet mehr Kontext zu den zuvor beobachteten Benutzernamen, ASN-Organisationen, Anwendungsnamen und Datenbanknamen für die zugehörige Datenbank. Jedem Einzelwert ist eine Anzahl zugeordnet, die angibt, wie oft dieser Wert bei einer erfolgreichen Anmeldung beobachtet wurde.

- Ungewöhnliches Verhalten (Konto-Kubernetes-Cluster, Kubernetes-Namespace und Kubernetes-Benutzername) – In diesem Abschnitt finden Sie zusätzliche Informationen zum profilierten Verhalten des Kubernetes-Clusters und des mit der Erkenntnis verbundenen Namespaces. Wenn ein Verhalten nicht als historisch identifiziert wird, bedeutet dies, dass das GuardDuty ML-Modell diesen Account, Cluster, Namespace oder Benutzernamen zuvor nicht auf diese Weise beobachtet hat. Zu den Informationen, die für diesen Abschnitt im Erkenntnisbereich verfolgt werden, gehören:
  - Benutzername – Der Benutzer, der die der Erkenntnis zugeordnete Kubernetes-API aufgerufen hat.
  - Impersonierter Nutzername – Der Benutzer, für den sich `username` ausgibt.
  - Namespace – Der Kubernetes-Namespace innerhalb des Amazon-EKS-Clusters, in dem die Aktion stattgefunden hat.
  - Benutzeragent – Der Benutzeragent, der dem Kubernetes-API-Aufruf zugeordnet ist. Der Benutzeragent ist die Methode, mit der der Aufruf ausgeführt wird, z. B. `kubectl`.
  - API – Die Kubernetes-API, die von `username` innerhalb des Amazon-EKS-Clusters aufgerufen wird.
  - ASN-Informationen – Die ASN-Informationen, wie Organisation und ISP, die der IP-Adresse des Benutzers zugeordnet sind, der diesen Aufruf tätigt.
  - Wochentag – Der Wochentag, an dem der Kubernetes-API-Aufruf getätigt wurde.

- Berechtigung [1] – Das Kubernetes-Verb und die Ressource, die auf Zugriff geprüft werden, um anzugeben, ob `username` die Kubernetes-API verwenden kann oder nicht.
- Servicekontoname [1] – Das dem Kubernetes-Workload zugeordnete Servicekonto, das dem Workload eine Identität verleiht.
- Registry[1] – Die Container-Registry, die dem Container-Image zugeordnet ist, das im Kubernetes-Workload bereitgestellt wird.
- Image[1] – Das Container-Image ohne die zugeordneten Tags und den Digest, das im Kubernetes-Workload bereitgestellt wird.
- Image-Präfix Config[1] – Das Image-Präfix mit aktivierter Container- und Workload-Sicherheitskonfiguration, z. B. `hostNetwork` oder `privileged`, für den Container, der das Image verwendet.
- Subjektname[1] – Die Subjekte, z. B. ein `user`, eine `group`, oder ein `serviceAccountName`, die an eine Referenzrolle in einem `RoleBinding` oder `ClusterRoleBinding` gebunden sind.
- Rollenname[1] – Der Name der Rolle, die an der Erstellung oder Änderung von Rollen oder der `roleBinding`-API beteiligt ist.

Volumenbezogene S3-Anomalien

In diesem Abschnitt werden die Kontextinformationen für volumenbasierte S3-Anomalien detailliert beschrieben. Die volumenbasierte Erkenntnis (Exfiltration:S3/AnomalousBehavior) überwacht, ob Benutzer ungewöhnlich viele S3-API-Aufrufe an die S3-Buckets tätigen, was auf eine mögliche Datenexfiltration hindeutet. Die folgenden S3-API-Aufrufe werden im Hinblick auf die volumenbasierte Erkennung von Anomalien überwacht.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

Die folgenden Metriken würden dabei helfen, eine Grundlage für das übliche Verhalten zu schaffen, wenn eine IAM-Entität auf einen S3-Bucket zugreift. Um Datenexfiltration zu erkennen, werden bei der volumenbasierten Erkennung von Anomalien alle Aktivitäten anhand der üblichen Verhaltensgrundlagen bewertet. Wählen Sie die Option Historisches Verhalten in den Abschnitten Ungewöhnliches Verhalten (Benutzeridentität), Beobachtetes Volumen (Benutzeridentität) und Beobachtetes Volumen (Bucket) aus, um jeweils die folgenden Metriken anzuzeigen.

- Anzahl der `s3-api-name`-API-Aufrufe, die von dem IAM-Benutzer oder der IAM-Rolle (je nachdem, welche ausgestellt wurde), der/die dem betroffenen S3-Bucket zugeordnet ist, in den letzten 24 Stunden durchgeführt wurden.
- Anzahl der `s3-api-name`-API-Aufrufe, die vom IAM-Benutzer oder von der IAM-Rolle (je nachdem, welche ausgestellt wurde) der/die allen S3-Buckets zugeordnet ist, in den letzen 24 Stunden durchgeführt wurden.
- Anzahl der `s3-api-name`-API-Aufrufe über alle IAM-Benutzer oder IAM-Rollen (je nachdem, welche ausgestellt wurden), die dem betroffenen S3-Bucket zugeordnet sind, in den letzten 24 Stunden durchgeführt wurden.

Anomalien aufgrund von RDS-Anmeldeaktivitäten

In diesem Abschnitt wird die Anzahl der Anmeldeversuche des ungewöhnlichen Akteurs detailliert beschrieben und nach den Ergebnissen der Anmeldeversuche gruppiert. Die Erkenntnistypen für RDS Protection identifizieren anomales Verhalten, indem sie die Anmeldeereignisse auf ungewöhnliche Muster von `successfulLoginCount`, `failedLoginCount` und `incompleteConnectionCount` überwachen.

- successfulLoginCount— Dieser Zähler stellt die Summe der erfolgreichen Verbindungen (richtige Kombination von Anmeldeattributen) dar, die der ungewöhnliche Akteur mit der Datenbankinstanz hergestellt hat. Zu den Anmeldeattributen gehören Benutzername, Passwort und Datenbankname.
- failedLoginCount— Dieser Zähler stellt die Summe der fehlgeschlagenen (erfolglosen) Anmeldeversuche dar, die unternommen wurden, um eine Verbindung zur Datenbankinstanz herzustellen. Dies weist darauf hin, dass ein oder mehrere Attribute der Anmeldekombination, wie Benutzername, Passwort oder Datenbankname, falsch waren.
- incompleteConnectionCount— Dieser Zähler stellt die Anzahl der Verbindungsversuche dar, die nicht als erfolgreich oder gescheitert eingestuft werden können. Diese Verbindungen werden geschlossen, bevor die Datenbank eine Antwort liefert. Beispielsweise Port-Scanning, bei dem der Datenbank-Port zwar verbunden ist, aber keine Information an die Datenbank gesendet wird, oder die Verbindung vor Abschluss der Anmeldung entweder erfolgreich oder fehlgeschlagen abgebrochen wurde.

GuardDuty-Erkenntnisformat

Wenn GuardDuty eine verdächtige oder unerwartete Aktivität in Ihrer AWS-Umgebung erkennt, erstellt der Service eine Erkenntnis. Eine Erkenntnis ist eine Benachrichtigung, die Details zu einem

von GuardDuty festgestellten potenziellen Sicherheitsrisiko enthält. Die Erkenntnisdetails enthalten Informationen darüber, was geschehen ist, welche AWS-Ressourcen an der verdächtigen Aktivität beteiligt waren und wann diese Aktivität stattfand, sowie weitere Informationen.

Eine der wichtigsten Informationen in den Ergebnisdetails ist der Ergebnistyp. Der Zweck des Ergebnistyps ist eine kurze und dennoch aussagekräftige Beschreibung des potenziellen Sicherheitsrisikos. So informiert Sie beispielsweise der GuardDuty-Ergebnistyp Recon:EC2/PortProbeUnprotectedPort darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung einen ungeschützten Port aufweist, der von einem potenziellen Angreifer untersucht wird.

GuardDuty verwendet das folgende Format für die verschiedenen Erkenntnistypen, die generiert werden:

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName.DetectionMechanism!Artifact

Jeder Teil dieses Formats steht für einen Aspekt eines Erkenntnistyps. Für diese Aspekte gibt es die folgenden Erklärungen:

- ThreatPurpose – Eine Beschreibung des Hauptzwecks einer Bedrohung oder eines potentiellen Angriffs. Im folgenden Abschnitt finden Sie eine vollständige Liste der Bedrohungszwecke von GuardDuty.
- ResourceTypeAffected – Dieser Wert gibt an, welche AWS-Ressource in diesem Ergebnis als potenzielles Ziel eines Angriffs ermittelt wurde. Derzeit kann GuardDuty Erkenntnisse für EC2-, S3-, IAM- und EKS-Ressourcen generieren.
- ThreatFamilyName – Eine Beschreibung der allgemeinen Bedrohung oder potenziell böswilliger Aktivitäten, die GuardDuty erkennt. Der Wert NetworkPortUnusual gibt beispielsweise an, dass eine EC2-Instance, die in der GuardDuty-Erkenntnis erkannt wurde, zuvor noch nicht über einen bestimmten Remote-Port kommuniziert hat, der ebenfalls in der Erkenntnis erkannt wurde.
- DetectionMechanism – beschreibt die Methode, mit der GuardDuty die Erkenntnis erkannt hat. Dies kann verwendet werden, um auf eine Variation eines gängigen Erkenntnistyps oder auf eine Erkenntnis hinzuweisen, für deren Erkennung GuardDuty einen bestimmten Mechanismus verwendet hat. Beispielsweise weist Backdoor:EC2/DenialOfService.Tcp darauf hin, dass eine Serviceverweigerung (DoS) über TCP erkannt wurde. Die UDP-Variante ist Backdoor:EC2/DenialOfService.Udp.

  Der Wert .Custom gibt an, dass GuardDuty die Erkenntnis anhand Ihrer benutzerdefinierten Bedrohungslisten erkannt hat, wohingegen .Reputation angibt, dass GuardDuty die Erkenntnis anhand eines Domain-Reputations-Punkte-Modells erkannt hat.

- Artefakt – Eine Beschreibung einer bestimmten Ressource eines Tools, das beim Angriff verwendet wird. So gibt beispielsweise DNS im Ergebnistyp CryptoCurrency:EC2/BitcoinTool.B!DNS an, dass eine EC2-Instance mit einer Domain kommuniziert, die mit Bitcoin in Verbindung steht.

Bedrohungszwecke

In GuardDuty beschreibt ein Bedrohungszweck den Hauptzweck einer Bedrohung, einen Angriffstyp oder ein Stadium eines potenziellen Angriffs. Beispielsweise deuten einige Bedrohungszwecke, wie Backdoor, auf einen Typ von Angriff hin. Einige Bedrohungszwecke, wie etwa Impact, stimmen jedoch mit den Taktiken von MITRE ATT&CK überein. Die MITRE-ATT&CK-Taktiken deuten auf verschiedene Phasen im Angriffszyklus eines Gegners hin. In der aktuellen Version von GuardDuty kann ThreatPurpose die folgenden Werte annehmen:

Backdoor

Dieser Wert gibt an, dass der Angriff eine AWS-Ressource kompromittiert hat und seinen eigenen Command-and-Control-Server (C&C-Server) kontaktieren kann, um weitere Anweisungen für schädigende Aktivitäten zu erhalten.

Verhalten

Dieser Wert gibt an, dass GuardDuty Aktivitäten oder Aktivitätsmuster erkennt, die sich vom normalen Verhalten einer bestimmten AWS-Ressource unterscheiden.

CredentialAccess

Dieser Wert gibt an, dass GuardDuty Aktivitätsmuster erkannt hat, anhand derer ein Angreifer Anmeldeinformationen wie Konto-IDs oder Passwörter aus Ihrer Umgebung stehlen kann. Dieser Bedrohungszweck basiert auf den MITRE-ATT&CK-Taktiken

Kryptowährung

Dieser Wert gibt an, dass GuardDuty erkannt hat, dass eine AWS-Ressource in Ihrer Umgebung Software hostet, die mit Kryptowährungen in Verbindung steht (z. B. Bitcoin).

DefenseEvasion

Dieser Wert zeigt an, dass GuardDuty Aktivitäten oder Aktivitätsmuster entdeckt hat, die ein Angreifer nutzen könnte, um sich beim Eindringen in Ihre Umgebung der Entdeckung zu entziehen. Dieser Bedrohungszweck basiert auf den MITRE-ATT&CK-Taktiken

Erkennung

Dieser Wert gibt an, dass GuardDuty Aktivitäten oder Aktivitätsmuster erkannt hat, anhand derer ein Angreifer sein Wissen über Ihre Systeme und internen Netzwerke erweitern kann. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Ausführung

Dieser Wert gibt an, dass GuardDuty erkannt hat, dass ein Angreifer möglicherweise versucht, bösartigen Code auszuführen, um das Netzwerk zu durchsuchen oder Daten zu stehlen. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Exfiltration

Dieser Wert gibt an, dass GuardDuty Aktivitäten oder Aktivitätsmuster erkannt hat, die ein Angreifer verwenden könnte, wenn er versucht, Daten aus Ihrem Netzwerk zu stehlen. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Auswirkung

Dieser Wert gibt an, dass GuardDuty Aktivitäten oder Aktivitätsmuster erkannt hat, die darauf hindeuten, dass ein Angreifer versucht, Ihre Systeme und Daten zu manipulieren, zu unterbrechen oder zu zerstören. Dieser Bedrohungszweck basiert auf den MITRE-ATT&CK-Taktiken

InitialAccess

Dieser Bedrohungszweck basiert auf den MITRE-ATT&CK-Taktiken

Penetrationstest

Manchmal führen die Eigentümer von AWS-Ressourcen oder ihre bevollmächtigten Vertreter absichtlich Tests mit AWS-Anwendungen durch, um Schwachstellen zu finden, z. B. offene Sicherheitsgruppen oder Zugriffsschlüssel, die zu viele Berechtigungen enthalten. Bei diesen Penetrationstests wird versucht, gefährdete Ressourcen zu erkennen und zu sperren, bevor sie von Angreifern entdeckt werden. Einige der von autorisierten Penetrationstestern verwendeten Tools sind jedoch kostenlos verfügbar und können daher auch von nicht autorisierten Benutzern oder Angreifern verwendet werden, um Analysetests durchzuführen. Obwohl GuardDuty den wahren Zweck einer solchen Aktivität nicht erkennen kann, zeigt der Pentest-Wert an, dass GuardDuty eine solche Aktivität erkennt, dass sie der Aktivität ähnelt, die von bekannten Penetrationstest-Tools erzeugt wird, und dass sie auf ein böswilliges Sondieren Ihres Netzwerks hindeuten könnte.

Persistenz

Dieser Wert gibt an, dass GuardDuty Aktivitäten oder Aktivitätsmuster erkannt hat, anhand derer ein Angreifer versuchen könnte, den Zugriff auf Ihre Systeme aufrechtzuerhalten, auch wenn der ursprüngliche Zugriffsweg unterbrochen ist. Dies könnte beispielsweise das Erstellen eines neuen IAM-Benutzers beinhalten, nachdem er über die kompromittierten Anmeldeinformationen eines vorhandenen Benutzers Zugriff erhalten hat. Wenn die Anmeldeinformationen des vorhandenen Benutzers gelöscht werden, behält der Angreifer den Zugriff auf den neuen Benutzer, der beim ursprünglichen Ereignis nicht erkannt wurde. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Richtlinie

Dieser Wert gibt an, dass Ihr AWS-Konto ein Verhalten zeigt, das den empfohlenen bewährten Sicherheitsmethoden widerspricht.

PrivilegeEscalation

Dieser Wert informiert Sie darüber, dass der betroffene Prinzipal in Ihrer AWS-Umgebung ein Verhalten an den Tag legt, das ein Angreifer nutzen könnte, um sich Zugriff auf Ihr Netzwerk auf höherer Ebene zu verschaffen. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Recon

Dieser Wert gibt an, dass GuardDuty Aktivitäten oder Aktivitätsmuster erkannt hat, anhand derer ein Angreifer Ihr Netzwerk auskundschaften kann, um festzustellen, wie er seinen Zugriff erweitern oder Ihre Ressourcen nutzen kann. Diese Aktivität kann beispielsweise das Aufspüren von Schwachstellen in Ihrer AWS-Umgebung umfassen, indem Ports untersucht, Benutzer und Datenbanktabellen aufgelistet werden usw.

Stealth

Dieser Wert gibt an, dass ein Angreifer aktiv versucht, seine Aktionen zu verbergen. Beispielsweise könnten sie einen anonymisierenden Proxyserver verwenden, was es extrem schwierig macht, die wahre Art der Aktivität einzuschätzen.

Trojan

Dieser Wert gibt an, dass der Angriff über Trojaner-Programme erfolgt, die im Hintergrund schädliche Aktivitäten durchführen. Es kann vorkommen, dass diese Software das Erscheinungsbild eines seriösen Programms annimmt. Es kann vorkommen, dass Benutzer diese

Software versehentlich ausführen. Die Software kann auch automatisch durch Ausnutzung einer Schwachstelle ausgeführt werden.

UnauthorizedAccess

Dieser Wert gibt an, dass GuardDuty verdächtige Aktivitäten oder Aktivitätsmuster einer unbefugten Person erkennt.

Generierung von Stichprobenbefunden in GuardDuty

Sie können mit Amazon Stichprobenergebnisse generieren GuardDuty , um die verschiedenen Befunde, die generiert werden GuardDuty können, zu visualisieren und zu verstehen. Wenn Sie Stichprobenergebnisse generieren, wird Ihre aktuelle Ergebnisliste mit einem Stichprobenergebnis für jeden unterstützten Befundtyp GuardDuty aufgefüllt.

Bei den generierten Beispielen handelt es sich um Näherungen, die mit Platzhalterwerten gefüllt sind. Diese Beispiele sehen möglicherweise anders aus als die tatsächlichen Ergebnisse für Ihre Umgebung, aber Sie können sie verwenden, um verschiedene Konfigurationen zu testen GuardDuty, z. B. Ihre CloudWatch Ereignisse oder Filter. Eine Liste der verfügbaren Werte für Erkenntnis-Typen finden Sie in der Tabelle Erkenntnistypen.

Informationen zum Generieren einiger häufiger Ergebnisse basierend auf simulierten Aktivitäten in Ihrer Umgebung finden Sie unter Automatische Generierung allgemeiner GuardDuty Ergebnisse unten.

Generieren von Beispielergebnissen über die GuardDuty Konsole oder API

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Beispiel-Erkenntnisse zu generieren.

> **Note**
>
> Die Konsolenmethode generiert jeweils einen Erkenntnistyp. Einzelne Beispiel-Erkenntnisse können nur über die API generiert werden.

Console

Gehen Sie wie folgt vor, um Beispielergebnisse zu erzeugen. Bei diesem Vorgang wird für jeden Befundtyp ein GuardDuty Stichprobenergebnis generiert.

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Klicken Sie auf der Seite Settings unter Sample findings auf Generate sample findings.
4. Wählen Sie im Navigationsbereich Findings aus. Die Beispiel-Erkenntnisse werden auf der Seite Aktuelle Erkenntnisse mit dem Präfix [SAMPLE] angezeigt.

API/CLI

Sie können über die CreateSampleFindingsAPI ein einzelnes Stichprobenergebnis generieren, GuardDuty das einem beliebigen Befundtyp entspricht. Die verfügbaren Werte für Suchtypen sind in der Erkenntnistypen Tabelle aufgeführt.

Dies ist nützlich für das Testen von CloudWatch Eventregeln oder für die Automatisierung auf der Grundlage von Ergebnissen. Das folgende Beispiel zeigt, wie Sie ein einzelnes Beispiel-Erkenntnis des `Backdoor:EC2/DenialOfService.Tcp`-Typs mithilfe der AWS CLI generieren können.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --finding-types Backdoor:EC2/DenialOfService.Tcp
```

Der Titel der mit diesen Methoden generierten Beispiel-Erkenntnisse beginnt in der Konsole immer mit [SAMPLE]. Beispiel-Erkenntnisse haben im Abschnitt additionalInfo der JSON-Erkenntnis-Details den Wert von `"sample": true`.

Automatische Generierung allgemeiner GuardDuty Ergebnisse

Sie können die folgenden Skripts verwenden, um automatisch mehrere allgemeine GuardDuty Ergebnisse zu generieren. Die guardduty-tester.template wird verwendet, AWS CloudFormation um eine isolierte Umgebung mit einem Bastion-Host, einer Amazon EC2 EC2-Testinstanz, auf die Sie über SSH zugreifen können, und zwei EC2-Zielinstanzen zu erstellen. Anschließend können Sie guardduty_tester.sh ausführen, um eine Interaktion zwischen der Tester-EC2-Instance, der Windows-EC2-Zielinstanz und der Linux-EC2-Zielinstanz zu starten, um fünf Arten häufiger Angriffe

zu simulieren, die anhand der generierten Ergebnisse erkennen und Sie darüber informieren können. GuardDuty

1. Voraussetzung ist, dass Sie die Option GuardDuty in dem Konto und der Region aktivieren, in der Sie guardduty-tester.template und guardduty_tester.sh ausführen möchten. Weitere Informationen zur Aktivierung finden Sie unter. GuardDuty Erste Schritte mit GuardDuty

   Außerdem müssen Sie ein neues EC2-Schlüsselpaar erstellen oder eine bestehendes EC2-Schlüsselpaar in jeder Region verwenden, in der Sie diese Skripte ausführen wollen. Dieses EC2-Schlüsselpaar wird als Parameter im guardduty-tester.template-Skript verwendet, mit dem Sie einen neuen Stack erstellen. CloudFormation Weitere Informationen über das Erzeugen von Schlüsselpaaren finden Sie unter Amazon-EC2-Schlüsselpaare.

2. Erstellen Sie CloudFormation mit guardduty-tester.template einen neuen Stack. Ausführliche Anweisungen zum Erstellen eines Stacks finden Sie unter Erstellen eines Stacks. Bevor Sie guardduty-tester.template ausführen, ändenr Sie es mit Werten für die folgenden Parameter ab: Stack Name zur Identifizierung Ihres neuen Stacks, Availability Zone, in der Sie den Stack ausführen möchten, und Key Pair, das Sie zum Starten der EC2-Instances verwenden können. Dann können Sie den entsprechenden privaten Schlüssel verwenden, um über SSH auf EC2-Instances zuzugreifen.

   Die Ausführung und Fertigstellung von guardduty-tester.template dauert ca. 10 Minuten. Es erstellt Ihre Umgebung und kopiert guardduty_tester.sh in Ihre Tester-EC2-Instance.

3. Wählen Sie in der AWS CloudFormation Konsole das Kontrollkästchen neben Ihrem neuen laufenden Stack aus. AWS CloudFormation Wählen Sie in der angezeigten Registerkartengruppe die Registerkarte Ausgabe. Notieren Sie die IP-Adressen, die dem Bastion-Host und der Tester-EC2-Instance zugeordnet sind. Sie benötigen diese beiden IP-Adressen, um über SSH auf die Tester-EC2-Instance zugreifen zu können.

4. Erstellen Sie den folgenden Eintrag in der Datei ~/.ssh/config, um sich über den Bastion-Host bei Ihrer Instance anzumelden.

```
Host bastion
        HostName {Elastic IP Address of Bastion}
        User ec2-user
        IdentityFile ~/.ssh/{your-ssh-key.pem}
Host tester
        ForwardAgent yes
        HostName {Local IP Address of RedTeam Instance}
        User ec2-user
```

```
        IdentityFile ~/.ssh/{your-ssh-key.pem}
        ProxyCommand ssh bastion nc %h %p
        ServerAliveInterval 240
```

Jetzt können Sie $ ssh tester aufrufen, um sich bei Ihrer Ziel-EC2-Instance anzumelden. Weitere Informationen zur Konfiguration und Verbindung zu EC2-Instances über Bastion-Hosts finden Sie unter https://aws.amazon.com/blogs/security/ securely-connect-to-linux - instances-running-in-a - private-amazon-vpc/.

5. Nachdem Sie eine Verbindung zur EC2-Testinstanz hergestellt haben, führen Sie guardduty_tester.sh aus, um die Interaktion zwischen Ihrem Tester und den EC2-Zielinstanzen zu initiieren, Angriffe zu simulieren und Ergebnisse zu generieren. GuardDuty

GuardDuty Schweregrade der Ergebnisse

Jedem GuardDuty Ergebnis ist ein Schweregrad und ein Wert zugewiesen, der das von unseren Sicherheitstechnikern festgestellte potenzielle Risiko für Ihr Netzwerk widerspiegelt. Der Wert des Schweregrads kann an beliebiger Stelle im Bereich von 1,0 bis 8,9 liegen, wobei höhere Werte auf ein höheres Sicherheitsrisiko hinweisen. Um Ihnen dabei zu helfen, eine Reaktion auf ein potenzielles Sicherheitsproblem zu finden, das durch ein Ergebnis hervorgehoben GuardDuty wird, wird dieser Bereich in die Schweregrade Hoch, Mittel und Niedrig unterteilt.

> **Note**
>
> Die Werte 0 und 9,0 bis 10,0 sind für die zukünftige Verwendung reserviert.

Im Folgenden sind die derzeit definierten Schweregrade und Werte für die GuardDuty Ergebnisse sowie allgemeine Empfehlungen für die einzelnen Ergebnisse aufgeführt:

Schweregrad	Wertebereich
Hoch	7,0 — 8,9
Der Schweregrad „Hoch“ weist darauf hin, dass die fragliche Ressource (z. B. eine EC2-Instance oder eine Gruppe von IAM-Benutzeranmeldeinformationen) erfolgreich angegriffen wurde und aktiv für unbefugte Zwecke verwendet wird.	

Schweregrad	Wertebereich
Es wird empfohlen, dass Sie Sicherheitsprobleme mit hohem Schweregrad als Priorität behandeln und sofortige Korrekturmaßnahmen ergreifen, um eine weitere unbefugte Nutzung Ihrer Ressourcen zu verhindern. Bereinigen oder beenden Sie Ihre EC2 Instance, oder rotieren Sie die IAM-Anmeldeinformationen. Weitere Informationen finden Sie unter Schritte zur Abhilfe.	
Mittel	4,0 - 6,9
Ein mittlerer Schweregrad weist auf verdächtige Aktivitäten hin, die vom normalerweise beobachte ten Verhalten abweichen und je nach Anwendungsfall auf eine Ressourcenkomprimettierung hinweisen können. Wir empfehlen Ihnen, die betroffene Ressource so bald wie möglich zu untersuchen. Die Schritte zur Abhilfe variieren je nach Ressource und Ergebnisfamilie. Im Allgemeinen sollten Sie jedoch prüfen, ob die Aktivität autorisiert ist und mit Ihrem Anwendungsfall übereinstimmt. Wenn Sie die Ursache nicht identifizieren oder nicht bestätigen können, dass die Aktivität autorisiert wurde, sollten Sie die Ressource als kompromittiert betrachten und zum Sichern der Ressource die Schritte zur Abhilfe befolgen. Hier sind einige Dinge, die Sie bei der Überprüfung eines Ergebnisses mittleren Schweregrades beachten sollten: • Prüfen Sie, ob ein autorisierter Benutzer neue Software installiert hat, die das Verhalten einer Ressource ändert (z. B. mehr Datenverkehr als normal zugelassen oder die Kommunikation über einen neuen Port aktiviert hat). • Überprüfen Sie, ob ein autorisierter Benutzer die Einstellungen für die Systemsteuerung (z. B. eine Sicherheitsgruppeneinstellung) geändert hat. • Führen Sie eine Virenprüfung der betroffenen Ressource durch, um nicht autorisierte Software zu erkennen. • Überprüfen Sie die Berechtigungen, die mit der betroffenen IAM-Rolle, dem Benutzer, der Gruppe oder den Anmeldeinformationen verbunden sind. Möglicherweise müssen diese geändert oder rotiert werden.	
Niedrig	1,0 - 3,9

Schweregrad	Wertebereich
Ein niedriger Schweregrad weist auf versuchte verdächtige Aktivitäten hin, die Ihr Netzwerk nicht gefährdet haben, z. B. einen Port-Scan oder einen fehlgeschlagenen Eindringungsversuch. Es gibt keine empfohlene Sofortmaßnahme, aber es lohnt sich, diesen Informationen Beachtung zu schenken, da dies möglicherweise darauf hindeutet, dass jemand nach Schwachstellen in Ihrem Netzwerk sucht.	

GuardDuty Aggregation finden

Alle Ergebnisse sind dynamisch, d. h., wenn eine neue Aktivität im Zusammenhang mit demselben Sicherheitsproblem GuardDuty erkannt wird, wird das ursprüngliche Ergebnis mit den neuen Informationen aktualisiert, anstatt ein neues Ergebnis zu generieren. Dieses Verhalten ermöglicht es Ihnen, laufende Probleme zu identifizieren, ohne mehrere ähnliche Berichte durchsehen zu müssen, und reduziert insgesamt das ausgelöste Rauschen durch Sicherheitsprobleme, die Ihnen bereits bekannt sind.

Zum Beispiel werden bei einer `UnauthorizedAccess:EC2/SSHBruteForce`-Erkenntnis mehrere Zugriffsversuche auf Ihre Instance unter derselben Erkenntnis-ID zusammengefasst, wodurch sich die Anzahl in den Details der Erkenntnis erhöht. Dies liegt daran, dass dieses Ergebnis ein einziges Sicherheitsproblem darstellt, wobei die Instance anzeigt, dass der SSH-Port auf der Instance nicht ordnungsgemäß vor dieser Art von Aktivität geschützt ist. Wenn jedoch SSH-Zugriffsaktivitäten GuardDuty erkannt werden, die auf eine neue Instanz in Ihrer Umgebung abzielen, wird ein neues Ergebnis mit einer eindeutigen Befund-ID erstellt, um Sie darauf hinzuweisen, dass mit der neuen Ressource ein Sicherheitsproblem verbunden ist.

Wenn eine Erkenntnis aggregiert wird, wird sie mit Informationen aus dem letzten Ereignis dieser Aktivität aktualisiert. Das bedeutet, dass im obigen Beispiel, wenn Ihre Instance das Ziel eines Brute-Force-Versuchs von einem neuen Akteur ist, die Erkenntnisdetails aktualisiert werden, um die Remote-IP der jüngsten Quelle wiederzugeben, und ältere Informationen ersetzt werden. Vollständige Informationen zu einzelnen Aktivitätsversuchen sind weiterhin in Ihren CloudTrail oder VPC Flow Logs verfügbar.

Die Kriterien, GuardDuty nach denen ein neues Ergebnis generiert wird, anstatt ein vorhandenes zu aggregieren, hängen vom Typ des Ergebnisses ab. Die Aggregationskriterien für jeden Ergebnistyp

werden von unseren Sicherheitstechnikern festgelegt, um Ihnen den besten Überblick über verschiedene Sicherheitsprobleme in Ihrem Konto zu geben.

Auffinden und Analysieren von Ergebnissen GuardDuty

Gehen Sie wie folgt vor, um Ihre GuardDuty Ergebnisse einzusehen und zu analysieren.

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Klicken Sie auf Ergebnisse und wählen Sie dann ein bestimmtes Ergebnis aus, um sich die Details anzeigen zu lassen.

   Die Details für jede Erkenntnis unterscheiden sich je nach Erkenntnistyp, betroffenen Ressourcen und Art der Aktivität. Weitere Informationen zu verfügbaren Ergebnisfeldern finden Sie unter Erkenntnisdetails.
3. (Optional) Wenn Sie eine Erkenntnis archivieren möchten, wählen Sie sie aus der Liste Ihrer Erkenntnisse aus und wählen Sie dann das Menü Aktionen. Wählen Sie dann Archivieren.

   Archivierte Erkenntnisse können angezeigt werden, indem Sie in der Dropdownliste Aktuell die Option Archiviert auswählen.

   Derzeit können GuardDuty Benutzer von GuardDuty Mitgliedskonten keine Ergebnisse archivieren.

   > **Important**
   >
   > Wenn Sie ein Ergebnis manuell mit dem oben beschriebenen Verfahren archivieren, werden alle nachfolgenden Vorkommen dieses Ergebnisses (die nach Abschluss der Archivierung generiert werden) der Liste Ihrer aktuellen Ergebnisse hinzugefügt. Wenn dieses Ergebnis nie in Ihrer aktuellen Liste angezeigt werden soll, können Sie es automatisch archivieren. Weitere Informationen finden Sie unter Unterdrückungsregeln.
4. (Optional) Zum Herunterzuladen eines Ergebnisses wählen Sie es in der Ergebnisliste aus und öffnen dann das Menü Aktionen. Wählen Sie dann Exportieren. Wenn Sie ein Ergebnis mit Export (Exportieren) exportieren, können Sie sein vollständiges JSON-Dokument einsehen.

> **Note**
>
> In einigen Fällen GuardDuty wird ihm bewusst, dass es sich bei bestimmten Ergebnissen um falsch positive Ergebnisse handelt, nachdem sie generiert wurden. GuardDuty stellt ein Konfidenzfeld in der JSON-Datei des Ergebnisses bereit und setzt dessen Wert auf Null. Auf diese Weise GuardDuty wissen Sie, dass Sie solche Ergebnisse getrost ignorieren können.

Erkenntnistypen

Informationen zu wichtigen Änderungen an den GuardDuty Befundtypen, einschließlich neu hinzugefügter oder zurückgezogener Befundtypen, finden Sie unterDokumentenverlauf für Amazon GuardDuty.

Hinweise zu Erkenntnis-Typen, die nun außer Betrieb genommen wurden, finden Sie unter Nicht mehr aktive Erkenntnistypen.

ECGuardDuty EC2Erkenntnistypen

Die folgenden Erkenntnisse sind spezifisch für Amazon-EC2-Ressourcen und haben immer einen Ressourcentyp von `Instance`. Der Schweregrad und die Details der Erkenntnisse unterscheiden sich je nach Ressourcenrolle, die angibt, ob die EC2-Instance das Ziel verdächtiger Aktivitäten war oder der Akteur, der die Aktivitäten durchführte.

Die hier aufgeführten Erkenntnisse beinhalten die Datenquellen und Modelle, die zur Generierung dieses Erkenntnistyps verwendet wurden. Weitere Informationen zu Datenquellen und Modellen finden Sie unter Grundlegende Datenquellen.

> **Note**
>
> Bei einigen EC2-Erkenntnissen fehlen möglicherweise Instance-Details, wenn die Instance bereits beendet wurde oder wenn der zugrunde liegende API-Aufruf Teil eines regionenübergreifenden API-Aufrufs war, der von einer EC2-Instance in einer anderen Region ausging.

Für alle EC2-Erkenntnisse wird empfohlen, die betreffende Ressource zu untersuchen, um festzustellen, ob sie sich erwartungsgemäß verhält. Wenn die Aktivität autorisiert ist, können Sie Unterdrückungsregeln oder Listen vertrauenswürdiger IP-Adressen verwenden, um Falschmeldungen für diese Ressource zu verhindern. Wenn die Aktivität unerwartet auftritt, besteht die bewährte Sicherheitsmethode darin, davon auszugehen, dass die Instance kompromittiert wurde, und die unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance beschriebenen Aktionen auszuführen.

Themen

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- Behavior:EC2/NetworkPortUnusual
- Behavior:EC2/TrafficVolumeUnusual
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- DefenseEvasion:EC2/UnusualDNSResolver
- DefenseEvasion:EC2/UnusualDoHActivity
- DefenseEvasion:EC2/UnusualDoTActivity
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce
- Recon:EC2/PortProbeEMRUnprotectedPort
- Recon:EC2/PortProbeUnprotectedPort
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS

- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/MetadataDNSRebind
- UnauthorizedAccess:EC2/RDPBruteForce
- UnauthorizedAccess:EC2/SSHBruteForce
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay

Backdoor:EC2/C&CActivity.B

Eine EC2-Instance fragt eine IP-Adresse ab, die einem bekannten Command-and-Control-Server zugeordnet wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Instance in Ihrer AWS-Umgebung eine IP-Adresse abfragt, der einem bekannten Command-and-Control (C&C)-Server zugeordnet ist. Die aufgeführte Instance ist möglicherweise kompromittiert. Command-and-control-Server sind Computer, die Befehle an Mitglieder eines Botnets senden.

Ein Botnet ist eine Sammlung von mit dem Internet verbundenen Geräten, zu denen PCs, Server, mobile Geräte und Geräte des Internets der Dinge gehören können, die mit einem allgemeinen Typ von Malware infiziert sind und von dieser kontrolliert werden. Botnets dienen häufig zum Verteilen von Malware und Sammeln von sich widerrechtlich angeeigneten Informationen, wie z. B. Kreditkartennummern. Je nach Zweck und Struktur des Botnets kann der C&C-Server auch den Befehl erteilen, einen DDoS (Distributed Denial of Service)-Angriff zu starten.

> **Note**
>
> Wenn die abgefragte IP log4j-bezogen ist, enthalten die Felder der zugehörigen Erkenntnis die folgenden Werte:

- service.additionalInfo .threatListName = Amazon
- service.additionalInfo.ThreatName = Log4j-bezogen

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Backdoor:EC2/C&CActivity.B!DNS

Eine EC2-Instance fragt einen Domainnamen ab, der einem bekannten Command-and-Control-Server zugeordnet wird.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Instance in Ihrer AWS-Umgebung einen Domainnamen abfragt, der einem bekannten Command-and-Control (C&C)-Server zugeordnet ist. Die aufgeführte Instance ist möglicherweise kompromittiert. Command-and-control-Server sind Computer, die Befehle an Mitglieder eines Botnets senden.

Ein Botnet ist eine Sammlung von mit dem Internet verbundenen Geräten, zu denen PCs, Server, mobile Geräte und Geräte des Internets der Dinge gehören können, die mit einem allgemeinen Typ von Malware infiziert sind und von dieser kontrolliert werden. Botnets dienen häufig zum Verteilen von Malware und Sammeln von sich widerrechtlich angeeigneten Informationen, wie z. B. Kreditkartennummern. Je nach Zweck und Struktur des Botnets kann der C&C-Server auch den Befehl erteilen, einen DDoS (Distributed Denial of Service)-Angriff zu starten.

> **Note**
>
> Wenn der abgefragte Domainname mit log4j zu tun hat, enthalten die Felder der zugehörigen Erkenntnis die folgenden Werte:
>
> - service.additionalInfo .threatListName = Amazon

- service.additionalInfo.ThreatName = Log4j-bezogen

> **Note**
>
> Um zu testen, wie diesen Erkenntnistyp GuardDuty generiert, können Sie eine DNS-Anfrage von Ihrer Instance (mit `dig` für Linux oder `nslookup` für Windows) gegen eine Testdomäne stellen`guarddutyc2activityb.com`.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Backdoor:EC2/DenialOfService.Dns

Das Verhalten einer EC2-Instance weist darauf hin, dass sie möglicherweise gerade für die Ausführung eines Denial-of-Service (DoS)-Angriffs mithilfe des DNS-Protokolls genutzt wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Dieses Ergebnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung eine große Menge ausgehenden DNS-Datenverkehrs generiert. Dies kann darauf hinweisen, dass die aufgeführte Instance kompromittiert ist und mithilfe des DNS-Protokolls zur Durchführung von denial-of-service (DoS-)Angriffen verwendet wird.

> **Note**
>
> Dieses Ergebnis erkennt nur DoS-Angriffe gegen öffentlich routingfähige IP-Adressen, die das primäre Ziel von DoS-Angriffen sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Backdoor:EC2/DenialOfService.Tcp

Das Verhalten einer EC2-Instance weist darauf hin, dass sie möglicherweise gerade für die Ausführung eines Denial-of-Service (DoS)-Angriffs mithilfe des TCP-Protokolls genutzt wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung eine große Menge ausgehenden TCP-Datenverkehrs generiert. Dies kann darauf hinweisen, dass die Instance kompromittiert ist und mithilfe des TCP-Protokolls zur Durchführung von denial-of-service (DoS-)Angriffen verwendet wird.

> **Note**
>
> Dieses Ergebnis erkennt nur DoS-Angriffe gegen öffentlich routingfähige IP-Adressen, die das primäre Ziel von DoS-Angriffen sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Backdoor:EC2/DenialOfService.Udp

Das Verhalten einer EC2-Instance weist darauf hin, dass sie möglicherweise gerade für die Ausführung eines Denial-of-Service (DoS)-Angriffs mithilfe des UDP-Protokolls genutzt wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung eine große Menge ausgehenden UDP-Datenverkehrs generiert. Dies kann darauf hinweisen, dass die aufgeführte Instance kompromittiert ist und mithilfe des UDP-Protokolls zur Durchführung von denial-of-service (DoS-)Angriffen verwendet wird.

> **Note**
>
> Dieses Ergebnis erkennt nur DoS-Angriffe gegen öffentlich routingfähige IP-Adressen, die das primäre Ziel von DoS-Angriffen sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

Das Verhalten einer EC2-Instance weist darauf hin, dass sie möglicherweise gerade für die Ausführung eines Denial-of-Service (DoS)-Angriffs mithilfe des UDP-Protokolls auf einem TCP-Port genutzt wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung eine große Menge ausgehenden UDP-Datenverkehrs generiert, der auf einen Port zielt, der normalerweise für die TCP-Kommunikation verwendet wird. Dies kann darauf hinweisen, dass die aufgeführte Instance kompromittiert ist und verwendet wird, um einen denial-of-service (DoS)-Angriff mit dem UDP-Protokoll auf einem TCP-Port durchzuführen.

> **Note**
>
> Dieses Ergebnis erkennt nur DoS-Angriffe gegen öffentlich routingfähige IP-Adressen, die das primäre Ziel von DoS-Angriffen sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Backdoor:EC2/DenialOfService.UnusualProtocol

Das Verhalten einer EC2-Instance weist darauf hin, dass sie möglicherweise gerade für die Ausführung eines Denial-of-Service (DoS)-Angriffs mithilfe eines ungewöhnlichen Protokolls genutzt wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung eine große Menge ausgehenden Datenverkehrs eines ungewöhnlichen Protokolltyps generiert, der normalerweise nicht von EC2-Instances verwendet wird (beispielsweise ein Internet Group Management Protocol). Dies kann darauf hinweisen, dass die Instance kompromittiert ist und verwendet wird, um denial-of-service (DoS)-Angriffe mit einem ungewöhnlichen Protokoll durchzuführen. Dieses Ergebnis erkennt nur DoS-Angriffe gegen öffentlich routingfähige IP-Adressen, die das primäre Ziel von DoS-Angriffen sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Backdoor:EC2/Spambot

Eine EC2-Instance zeigt ungewöhnliches Verhalten, indem sie mit einem Remote-Host auf Port 25 kommuniziert.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung mit einem Remote-Host auf Port 25 kommuniziert. Dieses Verhalten ist ungewöhnlich, da die betreffende EC2-Instance zuvor nicht über Port 25 kommuniziert hat. Port 25 wird in der Regel von Mailservern für die SMTP-Kommunikation verwendet. Dieses Ergebnis weist darauf hin, dass Ihre EC2-Instance für den Einsatz beim Versenden von Spam möglicherweise kompromittiert ist.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Behavior:EC2/NetworkPortUnusual

Eine EC2-Instance kommuniziert auf einem unüblichen Serverport mit einem Remote-Host.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung ein Verhalten zeigt, das von ihrem normalen Verhalten abweicht. Diese EC2-Instance hat früher nicht auf diesem Remote-Port kommuniziert.

> **Note**
>
> Wenn die EC2-Instance über Port 389 oder Port 1389 kommuniziert hat, wird der zugehörige Erkenntnis-Schweregrad auf Hoch geändert, und die Erkenntnisfelder enthalten den folgenden Wert:
>
> - service.additionalInfo.context = Möglicher log4j-Rückruf

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Behavior:EC2/TrafficVolumeUnusual

Eine EC2-Instance generiert ungewöhnlich große Mengen an Netzwerkdatenverkehr zu einem Remote-Host.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung ein Verhalten zeigt, das von ihrem normalen Verhalten abweicht. Diese EC2-Instance hat bisher nicht derart viel Datenverkehr an diesen Remote-Host gesendet.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

CryptoCurrency:EC2/BitcoinTool.B

Eine EC2-Instance fragt eine IP-Adresse ab, die mit einer Aktivität in Zusammenhang mit einer Kryptowährung steht.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung eine IP-Adresse abfragt, die mit einer Aktivität in Zusammenhang mit Bitcoin oder einer anderen Kryptowährung in Verbindung steht. Bitcoin ist ein weltweites Kryptowährungs- und digitales Zahlungssystem, das gegen andere Währungen, Produkte und Services eingetauscht werden kann. Bitcoin ist eine Belohnung für das Bitcoin-Mining und bei Bedrohungsakteuren sehr gefragt.

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2-Instance verwenden, um Kryptowährung zu minen oder zu verwalten, oder diese Instance anderweitig an der Blockchain-Aktivität beteiligt ist, könnte diese Erkenntnis erwartete Aktivitäten für Ihre Umgebung repräsentieren. Wenn dies in Ihrer AWS-Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `CryptoCurrency:EC2/BitcoinTool.B` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance sein, die an der Blockchain-Aktivität beteiligt ist. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn diese Aktivität unerwartet ist, ist Ihre Instance wahrscheinlich kompromittiert. Informationen dazu finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

CryptoCurrency:EC2/BitcoinTool.B!DNS

Eine EC2-Instance fragt einen Domainnamen ab, der mit einer Aktivität in Zusammenhang mit einer Kryptowährung steht.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung einen Domainnamen abfragt, die mit einer Aktivität in Zusammenhang mit Bitcoin oder einer anderen Kryptowährung in Verbindung steht. Bitcoin ist ein weltweites Kryptowährungs- und digitales Zahlungssystem, das gegen andere Währungen, Produkte und Services eingetauscht werden kann. Bitcoin ist eine Belohnung für das Bitcoin-Mining und bei Bedrohungsakteuren sehr gefragt.

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2-Instance verwenden, um Kryptowährung zu minen oder zu verwalten, oder diese Instance anderweitig an der Blockchain-Aktivität beteiligt ist, könnte diese Erkenntnis erwartete Aktivitäten für Ihre Umgebung repräsentieren. Wenn dies in Ihrer AWS-Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `CryptoCurrency:EC2/BitcoinTool.B!DNS` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance sein, die an der Blockchain-Aktivität beteiligt ist. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn diese Aktivität unerwartet ist, ist Ihre Instance wahrscheinlich kompromittiert. Informationen dazu finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

DefenseEvasion:EC2/UnusualDNSResolver

Eine Amazon-EC2-Instance kommuniziert mit einem ungewöhnlichen öffentlichen DNS-Resolver.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS-Umgebung ein Verhalten zeigt, das von ihrem normalen Verhalten abweicht. Diese EC2-Instance hat in letzter Zeit nicht mit diesem öffentlichen DNS-Resolver kommuniziert. Das Feld Unüblich im Bereich mit den Erkenntnisdetails in der GuardDuty Konsole kann Informationen über den abgefragten DNS-Resolver bereitstellen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

DefenseEvasion:EC2/UnusualDoHActivity

Eine Amazon-EC2-Instance führt eine ungewöhnliche DNS-über-HTTPS-Kommunikation (DoH) durch.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS-Umgebung ein Verhalten zeigt, das von ihrem normalen Verhalten abweicht. Diese EC2-Instance hat in letzter Zeit keine DNS-über-HTTPS-Kommunikation (DoH) mit diesem öffentlichen DoH-Server durchgeführt. Das Feld Ungewöhnlich in den Erkenntnisdetails kann Informationen über den abgefragten DoH-Server enthalten.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

DefenseEvasion:EC2/UnusualDoTActivity

Eine Amazon-EC2-Instance führt eine ungewöhnliche DNS-über-TLS-Kommunikation (DoT) durch.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung ein Verhalten zeigt, das von ihrem normalen Verhalten abweicht. Diese EC2-Instance hat in letzter Zeit keine DNS-über-TLS-Kommunikation (DoT) mit diesem öffentlichen DoT-Server durchgeführt. Das Feld Ungewöhnlich in den Erkenntnisdetails kann Informationen über den abgefragten DoT-Server enthalten.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Impact:EC2/AbusedDomainRequest.Reputation

Eine EC2-Instance fragt einen Domainnamen mit geringer Reputation ab, der mit bekanntermaßen missbrauchten Domains in Verbindung steht.

Standard-Schweregrad: Mittel

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS-Umgebung einen Domainnamen mit niedriger Reputation abfragt, der mit bekannten missbrauchten Domains oder IP-Adressen in Verbindung steht. Beispiele für missbrauchte Domains sind Top-

Level-Domainnamen (TLDs) und Second-Level-Domainnamen (2LDs), die kostenlose Subdomain-Registrierungen bieten, sowie dynamische DNS-Anbieter. Bedrohungsakteure nutzen diese Services in der Regel, um Domains kostenlos oder zu geringen Kosten zu registrieren. Bei Domains mit geringer Reputation in dieser Kategorie kann es sich auch um abgelaufene Domains handeln, die auf die Parking-IP-Adresse eines Registrars zurückgehen und daher möglicherweise nicht mehr aktiv sind. Bei einer Parking-IP leitet ein Registrar den Verkehr für Domains weiter, die mit keinem Service verknüpft wurden. Die aufgeführte Amazon-EC2-Instance kann kompromittiert sein, da Bedrohungsakteure diese Registrare oder Services häufig für C&C und die Verbreitung von Malware nutzen.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Impact:EC2/BitcoinDomainRequest.Reputation

Eine EC2-Instance fragt einen Domainnamen ab, der mit einer Aktivität in Zusammenhang mit einer Kryptowährung steht.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Dieses Ergebnis informiert Sie, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS-Umgebung einen Domainnamen mit niedriger Reputation abfragt, der mit einer Aktivität in Zusammenhang mit Bitcoin oder einer anderen Kryptowährung in Verbindung steht. Bitcoin ist ein weltweites Kryptowährungs- und digitales Zahlungssystem, das gegen andere Währungen, Produkte und Services eingetauscht werden kann. Bitcoin ist eine Belohnung für das Bitcoin-Mining und bei Bedrohungsakteuren sehr gefragt.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2-Instance verwenden, um Kryptowährung zu minen oder zu verwalten, oder diese Instance anderweitig an der Blockchain-Aktivität beteiligt ist, könnte diese Erkenntnis erwartete Aktivitäten für Ihre Umgebung repräsentieren. Wenn dies in Ihrer AWS-Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `Impact:EC2/BitcoinDomainRequest.Reputation` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance sein, die an der Blockchain-Aktivität beteiligt ist. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn diese Aktivität unerwartet ist, ist Ihre Instance wahrscheinlich kompromittiert. Informationen dazu finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Impact:EC2/MaliciousDomainRequest.Reputation

Eine EC2-Instance fragt eine Domain mit niedriger Reputation ab, die mit bekannten bösartigen Domains in Verbindung stehen.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS-Umgebung einen Domainnamen mit niedriger Reputation abfragt, der mit bekannten bösartigen Domains oder IP-Adressen in Verbindung stehen. Beispielsweise können Domains mit einer bekannten Sinkhole-IP-Adresse verknüpft sein. Sinkhole-Domains sind Domains, die zuvor von einem Bedrohungsakteur kontrolliert wurden, und Anfragen an sie können darauf hinweisen, dass die Instance kompromittiert wurde. Diese Domains können auch mit bekannten böswilligen Kampagnen oder Algorithmen zur Domain-Generierung korreliert sein.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Impact:EC2/PortSweep

Eine EC2-Instance untersucht einen Port auf einer großen Anzahl von IP-Adressen.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung einen Port auf einer großen Anzahl von öffentlich routingfähige IP-Adressen untersucht. Diese Art von Aktivität wird in der Regel verwendet, um anfällige Hosts zu finden, die ausgenutzt werden können. Im Bereich mit den Erkenntnisdetails in Ihrer GuardDuty Konsole wird nur die neueste Remote-IP-Adresse angezeigt

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Impact:EC2/SuspiciousDomainRequest.Reputation

Eine EC2-Instance fragt einen Domainnamen mit geringer Reputation ab, der aufgrund seines Alters oder seiner geringen Beliebtheit verdächtig ist.

Standard-Schweregrad: Niedrig

- Datenquelle: DNS-Protokolle

Dieses Ergebnis informiert Sie darüber, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS-Umgebung einen Domainnamen mit niedriger Reputation abfragt, bei dem der Verdacht besteht, dass er bösartig ist. Es wurden Merkmale dieser Domain festgestellt, die mit zuvor beobachteten bösartigen Domains übereinstimmten. Unser Reputationsmodell konnte sie jedoch nicht definitiv mit einer bekannten Bedrohung in Verbindung bringen. Diese Domains werden in der Regel neu beobachtet oder erhalten nur wenig Datenverkehr.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Impact:EC2/WinRMBruteForce

Eine EC2-Instance führt einen ausgehenden Brute-Force-Angriff für die Windows-Remoteverwaltung durch.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Schweregrad dieser Erkenntnis ist niedrig, wenn Ihre EC2-Instance das Ziel eines Brute-Force-Angriffs war. Der Schweregrad dieser Erkenntnis ist hoch, wenn Ihre EC2-Instance der zum Ausführen eines Brute-Force-Angriffs verwendete Akteur ist.

- Datenquelle: VPC-Flow-Protokolle

Dieses Ergebnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung einen Windows Remote Management (WinRM)-Brute-Force-Angriff durchführt, der darauf abzielt, Zugriff auf den Windows-Remote-Management-Service auf Windows-basierten Systemen zu erhalten.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Recon:EC2/PortProbeEMRUnprotectedPort

Eine EC2-Instance verfügt über einen ungeschützten EMR-bezogenen Port, der von einem bekannten böswilligen Host untersucht wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass ein EMR-bezogener sensibler Port auf der aufgelisteten EC2-Instance, der Teil eines Clusters in Ihrer AWS Umgebung ist, nicht von einer Sicherheitsgruppe, einer Zugriffskontrollliste (ACL) oder einer Host-Firewall wie Linux IPTables blockiert wird. Diese Erkenntnis informiert auch darüber, dass bekannte Kabel im Internet diesen Port aktiv untersuchen. Ports, die diese Erkenntnis auslösen können, z. B. Port 8088 (YARN Web-UI-Port), könnten potenziell für die Remote-Code-Ausführung genutzt werden.

Empfehlungen zur Abhilfe:

Sie sollten den offenen Zugang zu Ports auf Clustern aus dem Internet blockieren und den Zugang nur auf bestimmte IP-Adressen beschränken, die Zugang zu diesen Ports benötigen. Weitere Informationen finden Sie unter Sicherheitsgruppen für EMR-Cluster.

Recon:EC2/PortProbeUnprotectedPort

Eine EC2-Instance hat einen ungeschützten Port, der von einem bekannten böswilligen Host getestet wird.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Niedrig. Wenn jedoch der untersuchte Port von Elasticsearch (9200 oder 9300) verwendet wird, ist der Schweregrad der Erkenntnis Hoch.

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie, dass ein Port auf der aufgeführten EC2-Instance in Ihrer AWS-Umgebung nicht durch eine Sicherheitsgruppe, eine Zugriffssteuerungsliste (ACL) oder eine On-

Host-Firewall wie Linux IPTables blockiert ist und derzeit aktiv von bekannten Scannern im Internet untersucht wird.

Wenn der identifizierte ungeschützte Port 22 oder 3389 ist und Sie sich über diese Ports mit Ihrer Instance verbinden, können Sie die Exposition dennoch einschränken, indem Sie den Zugriff auf diese Ports nur für die IP-Adressen aus dem IP-Adressraum Ihres Unternehmensnetzwerks zulassen. Informationen zum Einschränken des Zugriffs auf Port 22 unter Linux finden Sie unter Autorisieren von eingehendem Datenverkehr für Linux-Instances. Informationen zum Einschränken des Zugriffs auf Port 3389 unter Windows finden Sie unter Autorisieren von eingehendem Datenverkehr für Windows-Instances.

GuardDuty generiert diese Erkenntnis nicht für die Ports 443 und 80.

Empfehlungen zur Abhilfe:

In einigen Fällen werden Instances absichtlich exponiert, weil sie beispielsweise Web-Server hosten. Wenn dies in Ihrer AWS-Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `Recon:EC2/PortProbeUnprotectedPort` verwenden. Das zweite Filterkriterium sollte den Instances entsprechen, die als Bastion-Host eingesetzt werden. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn diese Aktivität unerwartet ist, ist Ihre Instance wahrscheinlich kompromittiert. Informationen dazu finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Recon:EC2/Portscan

Eine EC2-Instance führt ausgehende Port-Scans an einem Remote-Host durch.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung an einem möglichen Port-Scan-Angriff beteiligt ist, da sie versucht, in kurzer Zeit Verbindungen zu

mehreren Ports herzustellen. Das Ziel eines Port-Scan-Angriffs ist die Ermittlung offener Ports, um zu ermitteln, welche Services und welches Betriebssystem der Computer ausführt.

Empfehlungen zur Abhilfe:

Diese Erkenntnis kann falsch positiv sein, wenn Anwendungen zur Schwachstellenbewertung auf EC2-Instances in der Umgebung bereitgestellt werden, weil diese Anwendungen Port-Scans durchführen, um Sie über falsch konfigurierte offene Ports zu informieren. Wenn dies in Ihrer AWS-Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `Recon:EC2/Portscan` verwenden. Das zweite Filterkriterium sollte den Instances entsprechen, die diese Tools zur Schwachstellenanalyse hosten. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn diese Aktivität unerwartet ist, ist Ihre Instance wahrscheinlich kompromittiert. Informationen dazu finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Trojan:EC2/BlackholeTraffic

Eine EC2-Instance versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, der ein bekanntes schwarzes Loch ist.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung möglicherweise kompromittiert wurde, da sie versucht, mit einer IP-Adresse eines schwarzen Lochs (oder eines Sinkholes) zu kommunizieren. Schwarze Löcher bezeichnen Orte im Netzwerk, an denen eingehender oder ausgehender Datenverkehr stillschweigend gelöscht wird, ohne die Quelle zu informieren, dass die Daten den vorgesehenen Empfänger nicht erreicht haben. Die IP-Adresse eines schwarzen Lochs gibt einen Hostcomputer an, der nicht ausgeführt wird, oder eine Adresse, der kein Host zugewiesen wurde.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Trojan:EC2/BlackholeTraffic!DNS

Eine EC2-Instance fragt einen Domainnamen ab, der an eine die IP-Adresse eines schwarzen Lochs weitergeleitet wird.

Standard-Schweregrad: Mittel

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung möglicherweise kompromittiert wurde, da sie einen Domainnamen abfragt, der an eine IP-Adresse eines schwarzen Lochs weitergeleitet wird. Schwarze Löcher bezeichnen Orte im Netzwerk, an denen eingehender oder ausgehender Datenverkehr stillschweigend gelöscht wird, ohne die Quelle zu informieren, dass die Daten den vorgesehenen Empfänger nicht erreicht haben.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Trojan:EC2/DGADomainRequest.B

Eine EC2-Instance fragt algorithmisch generierte Domänen ab. Solche Domänen werden häufig von Malware genutzt und können auf eine kompromittierte EC2-Instance hinweisen.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung versucht, DGA (Domain Generation Algorithms)-Domains abzufragen. Ihre EC2-Instance wurde möglicherweise kompromittiert.

DGAs werden verwendet, um in regelmäßigen Abständen eine große Anzahl an Domainnamen zu generieren, die als Rendezvous Points mit ihren Command-and-Control (C&C)-Servern verwendet werden können. Command-and-Control-Server sind Computer, die Befehle an die Mitglieder eines Botnets senden. Hierbei handelt es sich um eine Ansammlung von mit dem Internet verbundenen Geräten, die infiziert sind und von einer gängigen Malware kontrolliert werden. Die große Anzahl potenzieller Rendezvous Points erschwert ein effektives Stilllegen von Botnets, da infizierte Computer versuchen, einige dieser Domainnamen täglich zu kontaktieren, um Updates oder Befehle zu erhalten.

> **Note**
>
> Diese Erkenntnis basiert auf der Analyse von Domainnamen mit erweiterten Heuristiken und kann daher neue DGA-Domains identifizieren, die nicht in Bedrohungsdaten-Feeds vorhanden sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Trojan:EC2/DGADomainRequest.C!DNS

Eine EC2-Instance fragt algorithmisch generierte Domänen ab. Solche Domänen werden häufig von Malware genutzt und können auf eine kompromittierte EC2-Instance hinweisen.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung versucht, DGA (Domain Generation Algorithms)-Domains abzufragen. Ihre EC2-Instance wurde möglicherweise kompromittiert.

DGAs werden verwendet, um in regelmäßigen Abständen eine große Anzahl an Domainnamen zu generieren, die als Rendezvous Points mit ihren Command-and-Control (C&C)-Servern verwendet

werden können. Command-and-Control-Server sind Computer, die Befehle an die Mitglieder eines Botnets senden. Hierbei handelt es sich um eine Ansammlung von mit dem Internet verbundenen Geräten, die infiziert sind und von einer gängigen Malware kontrolliert werden. Die große Anzahl potenzieller Rendezvous Points erschwert ein effektives Stilllegen von Botnets, da infizierte Computer versuchen, einige dieser Domainnamen täglich zu kontaktieren, um Updates oder Befehle zu erhalten.

> **Note**
>
> Diese Erkenntnis basiert auf bekannten DGA-Domains aus GuardDutyden Bedrohungsinformationen-Feeds von .

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Trojan:EC2/DNSDataExfiltration

Eine EC2-Instance filtert Daten durch DNS-Abfragen heraus.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung Malware ausführt, die DNS-Abfragen für ausgehende Datenübertragungen verwendet. Diese Art der Datenübertragung weist auf eine kompromittierte Instance hin und kann zur Exfiltration von Daten führen. DNS-Datenverkehr wird in der Regel nicht durch Firewalls gesperrt. So kann beispielsweise Malware in einer kompromittierten EC2-Instance Daten verschlüsseln (z. B. Ihre Kreditkartennummer) und in einer DNS-Abfrage an einen entfernten DNS-Server senden, der von einem Angreifer gesteuert wird.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Trojan:EC2/DriveBySourceTraffic!DNS

Eine EC2-Instance fragt einen Domainnamen eines Remote-Host ab, der eine bekannte Quelle von Drive-By-Downloadangriffen ist.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung möglicherweise kompromittiert wurde, da Sie einen Domainnamen von einem Remote-Host abfragt, der eine bekannte Quelle von Drive-By-Download-Angriffen ist. Hierbei handelt es sich um unbeabsichtigte Downloads von Computersoftware aus dem Internet, die eine automatische Installation von Viren, Spyware oder Malware auslösen kann.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Trojan:EC2/DropPoint

Eine EC2-Instance versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, von dem bekannt ist, dass er Anmeldedaten und andere mithilfe von Malware gestohlene Daten enthält.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie, dass eine EC2-Instance in Ihrer AWS-Umgebung versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, von dem bekannt ist, dass er Anmeldeinformationen und andere mithilfe von Malware gestohlene Daten enthält.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Trojan:EC2/DropPoint!DNS

Eine EC2-Instance fragt einen Domainnamen eines Remote-Hosts ab, von dem bekannt ist, dass er Anmeldedaten und andere mithilfe von Malware gestohlene Daten enthält.

Standard-Schweregrad: Mittel

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie, dass eine EC2-Instance in Ihrer AWS-Umgebung einen Domainnamen eines Remote-Hosts abfragt, von dem bekannt ist, dass er Anmeldeinformationen und andere mithilfe von Malware gestohlene Daten enthält.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Trojan:EC2/PhishingDomainRequest!DNS

Eine EC2-Instance fragt Domänen ab, die an Phishing-Angriffen beteiligt sind. Ihre EC2-Instance wurde möglicherweise kompromittiert.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung versucht, eine Domain abzufragen, die an Phishing-Angriffen beteiligt ist. Phishing-Domains werden von jemandem eingerichtet, der sich als rechtmäßige Institution ausgibt, um Personen dazu zu bringen, sensible Daten bereitzustellen, wie beispielsweise personenbezogene Informationen, Bank- und Kreditkartendaten oder Passwörter. Ihre EC2-Instance versucht möglicherweise, sensible Daten abzurufen, die auf einer Phishing-Website gespeichert sind, oder sie versucht möglicherweise, eine Phishing-Website einzurichten. Ihre EC2-Instance wurde möglicherweise kompromittiert.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

Eine EC2-Instance stellt Verbindungen zu einer IP-Adresse auf einer benutzerdefinierten Bedrohungsliste her.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung mit einer IP-Adresse kommuniziert, die auf einer von Ihnen hochgeladenen Bedrohungsliste steht. In GuardDuty besteht eine Bedrohungsliste aus bekannten schädlichen IP-Adressen. GuardDuty generiert Ergebnisse basierend auf hochgeladenen Bedrohungslisten. Die Bedrohungsliste, die zum Generieren dieser Suche verwendet wird, wird in den Details der Suche aufgeführt.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

UnauthorizedAccess:EC2/MetadataDNSRebind

Eine EC2-Instance führt DNS-Abrufe durch, die in den Instance-Metadatenservice aufgelöst werden.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung eine Domain abfragt, die in die IP-Adresse der EC2-Metadaten (169.254.169.254) aufgelöst wird. Eine solche DNS-Abfrage kann darauf hinweisen, dass die Instance das Ziel einer DNS-Neubindung-Technik ist. Diese Technik kann verwendet werden, um Metadaten von einer EC2-Instance abzurufen, einschließlich der mit der Instance verknüpften IAM-Anmeldeinformationen.

Bei der DNS-Neubindung wird eine Anwendung, die auf der EC2-Instance läuft, dazu gebracht, Rückgabedaten von einer URL zu laden, wobei der Domainname in der URL in die IP-Adresse der EC2-Metadaten (169.254.169.254) aufgelöst wird. Dies bewirkt, dass die Anwendung auf EC2-Metadaten zugreift und sie möglicherweise für den Angreifer verfügbar macht.

Der Zugriff auf EC2-Metadaten mit DNS-Neubindung ist nur möglich, wenn auf der EC2-Instance eine anfällige Anwendung ausgeführt wird, die das Einfügen von URLs ermöglicht, oder wenn ein menschlicher Benutzer in einem Webbrowser, der auf der EC2-Instance ausgeführt wird, auf die URL zugreift.

Empfehlungen zur Abhilfe:

Prüfen Sie als Reaktion auf diese Erkenntnis, ob auf der EC2-Instance eine anfällige Anwendung ausgeführt wird, oder ob ein menschlicher Benutzer über einen Browser auf die im Ergebnis angegebene Domain zugegriffen hat. Wenn die Ursache eine anfällige Anwendung ist, beheben Sie die Schwachstelle. Wenn ein Benutzer die identifizierte Domain aufgerufen hat, blockieren Sie die Domain oder verhindern Sie, dass Benutzer darauf zugreifen. Wenn Sie in dieser Erkenntnis einen Zusammenhang mit einem der obigen Fälle feststellen, sollten Sie die der EC2-Instance zugeordnete Sitzung widerrufen.

Einige AWS-Kunden ordnen die IP-Adresse der Metadaten absichtlich einem Domainnamen auf ihren autoritativen DNS-Servern zu. Wenn dies in Ihrer -Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `UnauthorizedAccess:EC2/MetaDataDNSRebind` verwenden. Das zweite Filterkriterium sollte die DNS-Anforderungs-Domain sein, und der Wert sollte mit der Domain übereinstimmen, die Sie der Metadaten-IP-Adresse zugeordnet haben (169.254.169.254). Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

UnauthorizedAccess:EC2/RDPBruteForce

Eine EC2-Instance war an RDP-Brute-Force-Angriffen beteiligt.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Schweregrad dieser Erkenntnis ist niedrig, wenn Ihre EC2-Instance das Ziel eines Brute-Force-Angriffs war. Der Schweregrad dieser Erkenntnis ist hoch, wenn Ihre EC2-Instance der zum Ausführen eines Brute-Force-Angriffs verwendete Akteur ist.

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung an einem Brute-Force-Angriff beteiligt war, der auf die Beschaffung von Passwörtern für RDP-Services auf Windows-basierten Systemen ausgerichtet war. Dies kann auf einen unbefugten Zugriff auf Ihre AWS-Ressourcen hinweisen.

Empfehlungen zur Abhilfe:

Wenn die Ressourcenrolle Ihrer Instance `ACTOR` lautet, bedeutet dies, dass Ihre Instance zum Ausführen von RDP-Brute-Force-Angriffen verwendet wurde. Außer, wenn diese Instance einen legitimen Grund hat, die IP-Adresse zu kontaktieren, die als `Target` aufgeführt ist, wird empfohlen, davon auszugehen, dass Ihre Instance kompromittiert wurde, und die in Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance aufgeführten Maßnahmen zu ergreifen.

Wenn die Ressourcenrolle Ihrer Instance `TARGET` lautet, kann dieses Problem behoben werden, indem Sie Ihren RDP-Port mit Hilfe von Sicherheitsgruppen, ACLs oder Firewalls nur für vertrauenswürdige IPs sichern. Weitere Informationen finden Sie unter Tipps zur Sicherung Ihrer EC2-Instances (Linux).

UnauthorizedAccess:EC2/SSHBruteForce

Eine EC2-Instance war an SSH-Brute-Force-Angriffen beteiligt.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Schweregrad dieser Erkenntnis ist niedrig, wenn ein Brute-Force-Angriff auf eine Ihrer EC2-Instances abzielt. Der Schweregrad dieser Erkenntnis ist hoch, wenn Ihre EC2-Instance verwendet wird, um einen Brute-Force-Angriff durchzuführen.

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung an einem Brute-Force-Angriff beteiligt war, der auf die Beschaffung von Passwörtern für SSH-Services auf Linux-basierten Systemen ausgerichtet war. Dies kann auf einen unbefugten Zugriff auf Ihre AWS-Ressourcen hinweisen.

> **Note**
>
> Dieses Ergebnis wird nur über den -Überwachungsdatenverkehr auf Port 22 generiert. Wenn Ihre SSH-Services konfiguriert sind, um andere Ports zu verwenden, wird dieses Ergebnis nicht generiert.

Empfehlungen zur Abhilfe:

Wenn das Ziel des versuchten Brute-Force-Angriffs ein Bastion-Host ist, kann dies das erwartete Verhalten für die betreffende AWS-Umgebung darstellen. In diesem Fall sollten Sie für dieses Ergebnis eine Unterdrückungsregel einrichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `UnauthorizedAccess:EC2/SSHBruteForce` verwenden. Das zweite Filterkriterium sollte den Instances entsprechen, die als Bastion-Host eingesetzt werden. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn diese Aktivitäten für Ihre Umgebung nicht erwartet werden und die Ressourcenrolle Ihrer Instance `TARGET` lautet, kann diese Erkenntnis behoben werden, indem Sie Ihren SSH-Port mit

Hilfe von Sicherheitsgruppen, ACLs oder Firewalls nur für vertrauenswürdige IPs sichern. Weitere Informationen finden Sie unter Tipps zur Sicherung Ihrer EC2-Instances (Linux).

Wenn die Ressourcenrolle Ihrer Instance `ACTOR` lautet, bedeutet dies, dass die Instance zum Ausführen von SSH-Brute-Force-Angriffen verwendet wurde. Außer, wenn diese Instance einen legitimen Grund hat, die IP-Adresse zu kontaktieren, die als `Target` aufgeführt ist, wird empfohlen, davon auszugehen, dass Ihre Instance kompromittiert wurde, und die in Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance aufgeführten Maßnahmen zu ergreifen.

UnauthorizedAccess:EC2/TorClient

Ihre EC2-Instance stellt Verbindungen mit einem Tor Guard oder einem Authority-Knoten her.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung Verbindungen zu einem Tor-Guard oder einem Authority-Knoten herstellt. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor Guards und Authority-Knoten fungieren als erste Gateways in ein Tor-Netzwerk. Dieser Datenverkehr kann darauf hinweisen, dass diese EC2-Instance als Client in einem Tor-Netzwerk fungiert. Diese Erkenntnis kann auf einen unbefugten Zugriff auf die AWS-Ressourcen hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

UnauthorizedAccess:EC2/TorRelay

Ihre EC2-Instance stellt Verbindungen mit einem Tor-Netzwerk als Tor-Relais her.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung Verbindungen zu einem Tor-Netzwerk auf eine Weise herstellt, die darauf hindeutet, dass sie als Tor-Relay fungiert. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor-Relays erhöhen die Anonymität der Kommunikation, indem sie den möglicherweise illegalen Datenverkehr des Kunden von einem Tor-Relay zu einem anderen weiterleiten.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

GuardDuty IAM-Erkenntnistypen

Die folgenden Erkenntnisse beziehen sich auf IAM-Entitäten und Zugriffsschlüssel und weisen immer den Ressourcentyp `AccessKey` auf. Der Schweregrad und die Details der Erkenntnisse unterscheiden sich je nach Erkenntnistyp.

Die hier aufgeführten Erkenntnisse beinhalten die Datenquellen und Modelle, die zur Generierung dieses Erkenntnistyps verwendet wurden. Weitere Informationen finden Sie unter Grundlegende Datenquellen.

Für alle Erkenntnisse im Zusammenhang mit IAM empfehlen wir, dass Sie die fragliche Entität untersuchen und sicherstellen, dass ihre Berechtigungen der bewährten Methode der geringsten Berechtigung entsprechen. Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen zur Behebung von Erkenntnissen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Themen

- Persistence:IAMUser/AnomalousBehavior
- Policy:IAMUser/RootCredentialUsage
- PrivilegeEscalation:IAMUser/AnomalousBehavior
- Recon:IAMUser/MaliciousIPCaller
- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/TorIPCaller

CredentialAccess:IAMUser/AnomalousBehavior

Eine API, die für den Zugriff auf eine AWS Umgebung verwendet wird, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignis

Diese Erkenntnis informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API-Anfrage beobachtet wurde. Diese Erkenntnis kann eine einzelne API oder eine Reihe verwandter API-Anfragen beinhalten, die in unmittelbarer Nähe von einer einzelnen Benutzeridentität gestellt wurden. Die beobachtete API wird häufig mit der Phase des Zugriffs auf Anmeldeinformationen in Verbindung gebracht, wenn ein Angreifer versucht, Passwörter, Benutzernamen und Zugriffsschlüssel für Ihre Umgebung zu sammeln. Die APIs `GetPasswordData`, `GetSecretValue` und `GenerateDbAuthToken` sind nicht in dieser Kategorie enthalten.

Diese API-Anfrage wurde durch GuardDutydas Machine Learning (ML)-Modell zur Anomalieerkennung von als ungewöhnlich identifiziert. Das ML-Modell wertet alle API-Anfragen an

Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde. Einzelheiten darüber, welche Faktoren der API-Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

DefenseEvasion:IAMUser/AnomalousBehavior

Eine API, die zur Umgehung von Abwehrmaßnahmen verwendet wird, wurde auf anomale Weise aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignis

Diese Erkenntnis informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API-Anfrage beobachtet wurde. Diese Erkenntnis kann eine einzelne API oder eine Reihe verwandter API-Anfragen beinhalten, die in unmittelbarer Nähe von einer einzelnen Benutzeridentität gestellt wurden. Die beobachtete API wird häufig mit Umgehungstaktiken in Verbindung gebracht, bei denen ein Gegner versucht, seine Spuren zu verwischen und nicht entdeckt zu werden. Bei APIs in dieser Kategorie handelt es sich in der Regel um Lösch-, Deaktivierungs- oder Stoppvorgänge wie `DeleteFlowLogs`, `DisableAlarmActions` oder `StopLogging`.

Diese API-Anfrage wurde durch GuardDutydas Machine Learning (ML)-Modell zur Anomalieerkennung von als ungewöhnlich identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde. Einzelheiten darüber, welche Faktoren der API-Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Discovery:IAMUser/AnomalousBehavior

Eine API, die häufig zum Auffinden von Ressourcen verwendet wird, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Niedrig

- Datenquelle: CloudTrail Verwaltungsereignis

Diese Erkenntnis informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API-Anfrage beobachtet wurde. Diese Erkenntnis kann eine einzelne API oder eine Reihe verwandter API-Anfragen beinhalten, die in unmittelbarer Nähe von einer einzelnen Benutzeridentität gestellt wurden. Die beobachtete API wird häufig mit der Erkennungsphase eines Angriffs in Verbindung gebracht, wenn ein Angreifer Informationen sammelt, um festzustellen, ob Ihre AWS Umgebung für einen umfassenderen Angriff anfällig ist. APIs in dieser Kategorie sind in der Regel Get-, Describe- oder List-Vorgänge wie `DescribeInstances`, `GetRolePolicy` oder `ListAccessKeys`.

Diese API-Anfrage wurde durch GuardDutydas Machine Learning (ML)-Modell zur Anomalieerkennung von als ungewöhnlich identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde. Einzelheiten darüber, welche Faktoren der API-Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Exfiltration:IAMUser/AnomalousBehavior

Eine API, die häufig zum Sammeln von Daten aus einer AWS Umgebung verwendet wird, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Verwaltungsereignis

Diese Erkenntnis informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API-Anfrage beobachtet wurde. Diese Erkenntnis kann eine einzelne API oder eine Reihe verwandter API-Anfragen beinhalten, die in unmittelbarer Nähe von einer einzelnen Benutzeridentität gestellt wurden. Die beobachtete API wird üblicherweise mit Exfiltrationstaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten aus Ihrem Netzwerk zu sammeln, indem er sie verpackt und verschlüsselt, um eine Entdeckung zu vermeiden. APIs für diesen Erkenntnistyp sind Verwaltungsvorgänge (Steuerebene) und beziehen sich in der Regel auf S3, Snapshots und Datenbanken wie `PutBucketReplication`, `CreateSnapshot` oder `RestoreDBInstanceFromDBSnapshot`.

Diese API-Anfrage wurde durch GuardDutydas Machine Learning (ML)-Modell zur Anomalieerkennung von als ungewöhnlich identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde. Einzelheiten darüber, welche Faktoren der API-Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Impact:IAMUser/AnomalousBehavior

Eine API, die häufig zur Manipulation von Daten oder Prozessen in einer AWS Umgebung verwendet wird, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Verwaltungsereignis

Diese Erkenntnis informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API-Anfrage beobachtet wurde. Diese Erkenntnis kann eine einzelne API oder eine Reihe verwandter API-Anfragen beinhalten, die in unmittelbarer Nähe von einer einzelnen Benutzeridentität gestellt wurden. Die beobachtete API wird in der Regel mit Angriffstaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, den Betrieb zu stören und Daten in Ihrem Konto zu manipulieren, zu unterbrechen oder zu zerstören. APIs für diese Art der Suche sind in der Regel Lösch-, Aktualisierungs- oder Stellvorgänge wie `DeleteSecurityGroup`, `UpdateUser` oder `PutBucketPolicy`.

Diese API-Anfrage wurde durch GuardDutydas Machine Learning (ML)-Modell zur Anomalieerkennung von als ungewöhnlich identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde. Einzelheiten darüber, welche Faktoren der API-Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

InitialAccess:IAMUser/AnomalousBehavior

Eine API, die häufig verwendet wird, um unbefugten Zugriff auf eine AWS Umgebung zu erhalten, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignis

Diese Erkenntnis informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API-Anfrage beobachtet wurde. Diese Erkenntnis kann eine einzelne API oder eine Reihe verwandter API-Anfragen beinhalten, die in unmittelbarer Nähe von einer einzelnen Benutzeridentität gestellt wurden. Die beobachtete API wird häufig mit der ersten Zugriffsphase eines Angriffs in Verbindung gebracht, wenn ein Angreifer versucht, Zugriff auf Ihre Umgebung zu erhalten. APIs dieser Kategorie sind in der Regel Get-Token- oder Session-Vorgänge wie `GetFederationToken`, `StartSession` oder `GetAuthorizationToken`.

Diese API-Anfrage wurde durch GuardDutydas Machine Learning (ML)-Modell zur Anomalieerkennung von als ungewöhnlich identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde. Einzelheiten darüber, welche Faktoren der API-Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

PenTest:IAMUser/KaliLinux

Eine API wurde von einem Kali-Linux-Computer aus aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignis

Diese Erkenntnis informiert Sie darüber, dass ein Computer, auf dem Kali Linux ausgeführt wird, API-Aufrufe mit Anmeldeinformationen durchführt, die zum aufgelisteten AWS Konto in Ihrer Umgebung gehören. Kali Linux ist ein beliebtes Tool für Penetrationstests, das von Sicherheitsexperten verwendet wird, um Schwachstellen in EC2-Instances zu erkennen, für die Patches erforderlich sind. Angreifer verwenden dieses Tool auch, um EC2-Konfigurationsschwächen zu finden und sich unbefugten Zugriff auf Ihre AWS Umgebung zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

PenTest:IAMUser/ParrotLinux

Eine API wurde von einem Parrot-Security-Linux-Computer aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignis

Diese Erkenntnis informiert Sie darüber, dass ein Computer, auf dem Parrot Security Linux ausgeführt wird, API-Aufrufe mit Anmeldeinformationen durchführt, die zum aufgelisteten AWS Konto in Ihrer Umgebung gehören. Parrot Security Linux ist ein beliebtes Tool für Penetrationstests, das von Sicherheitsexperten verwendet wird, um Schwachstellen in EC2-Instances zu erkennen, für die Patches erforderlich sind. Angreifer verwenden dieses Tool auch, um EC2-Konfigurationsschwächen zu finden und sich unbefugten Zugriff auf Ihre AWS Umgebung zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

PenTest:IAMUser/PentooLinux

Eine API wurde von einem Pentoo-Linux-Computer aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignis

Diese Erkenntnis informiert Sie darüber, dass ein Computer, auf dem Pentoo Linux ausgeführt wird, API-Aufrufe mit Anmeldeinformationen durchführt, die zum aufgelisteten AWS Konto in Ihrer Umgebung gehören. Pentoo Linux ist ein beliebtes Tool für Penetrationstests, das von Sicherheitsexperten verwendet wird, um Schwachstellen in EC2-Instances zu erkennen, für die Patches erforderlich sind. Angreifer verwenden dieses Tool auch, um EC2-Konfigurationsschwächen zu finden und sich unbefugten Zugriff auf Ihre AWS Umgebung zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Persistence:IAMUser/AnomalousBehavior

Eine API, die häufig verwendet wird, um unbefugten Zugriff auf eine AWS Umgebung aufrechtzuerhalten, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignis

Diese Erkenntnis informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API-Anfrage beobachtet wurde. Diese Erkenntnis kann eine einzelne API oder eine Reihe verwandter API-Anfragen beinhalten, die in unmittelbarer Nähe von einer einzelnen Benutzeridentität gestellt wurden. Die beobachtete API wird häufig mit Persistenztaktiken in Verbindung gebracht, bei denen sich ein Angreifer Zugriff auf Ihre Umgebung verschafft hat und versucht, diesen Zugriff aufrechtzuerhalten. APIs in dieser Kategorie sind in der Regel Erstellungs-, Import- oder Änderungsvorgänge wie `CreateAccessKey`, `ImportKeyPair` oder `ModifyInstanceAttribute`.

Diese API-Anfrage wurde durch GuardDutydas Machine Learning (ML)-Modell zur Anomalieerkennung von als ungewöhnlich identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde. Einzelheiten darüber, welche Faktoren der API-Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Policy:IAMUser/RootCredentialUsage

Eine API wurde über Root-Benutzer-Anmeldeinformationen aufgerufen.

Standard-Schweregrad: Niedrig

- Datenquelle: CloudTrail Verwaltungsereignisse oder CloudTrail Datenereignisse

Diese Erkenntnis informiert Sie darüber, dass die Root-Benutzer-Anmeldeinformationen des in Ihrer Umgebung angeführten AWS-Konto -Kontos verwendet werden, um Anforderungen an AWS -Services zu erstellen. Es wird empfohlen, dass Benutzer niemals Anmeldeinformationen für Root-Benutzer verwenden, um auf - AWS Services zuzugreifen. Stattdessen sollte auf AWS Services

zugegriffen werden, indem temporäre Anmeldeinformationen mit den geringsten Berechtigungen von AWS Security Token Service (STS) verwendet werden. Für Situationen, in denen AWS STS nicht unterstützt wird, werden IAM-Benutzeranmeldeinformationen empfohlen. Weitere Informationen finden Sie unter Bewährte Methoden für IAM.

> **Note**
>
> Wenn die S3-Bedrohungserkennung für das Konto aktiviert ist, kann diese Erkenntnis als Reaktion auf Versuche generiert werden, S3-Datenebenenvorgänge auf S3-Ressourcen unter Verwendung der Anmeldeinformationen des Root-Benutzers der AWS-Kontoauszuführen. Der verwendete API-Aufruf wird in den Erkenntnisdetails aufgeführt. Wenn die S3-Bedrohungserkennung nicht aktiviert ist, kann diese Erkenntnis nur durch Ereignisprotokoll-APIs ausgelöst werden. Weitere Informationen zur S3-Bedrohungserkennung finden Sie unter S3 Protection.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

PrivilegeEscalation:IAMUser/AnomalousBehavior

Eine API, die häufig verwendet wird, um allgemeine Berechtigungen für eine AWS Umgebung zu erhalten, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API-Anfrage beobachtet wurde. Diese Erkenntnis kann eine einzelne API oder eine Reihe verwandter API-Anfragen beinhalten, die in unmittelbarer Nähe von einer einzelnen Benutzeridentität gestellt wurden. Die beobachtete API wird häufig mit Taktiken zur Eskalation von Rechten in Verbindung gebracht, bei denen ein Angreifer versucht, Berechtigungen auf höherer Ebene für eine Umgebung zu erlangen. APIs in dieser Kategorie beinhalten in der Regel Vorgänge, die IAM-Richtlinien, Rollen und Benutzer ändern, wie `AssociateIamInstanceProfile`, `AddUserToGroup` oder `PutUserPolicy`.

Diese API-Anfrage wurde durch GuardDutydas Machine Learning (ML)-Modell zur Anomalieerkennung von als ungewöhnlich identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Das ML-Modell verfolgt verschiedene Faktoren der API-Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifische API, die angefordert wurde. Einzelheiten darüber, welche Faktoren der API-Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Recon:IAMUser/MaliciousIPCaller

Eine API wurde von einer bekannten böswilligen IP-Adresse aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie, dass ein API-Vorgang, der AWS -Ressourcen auflisten oder beschreiben kann, von einer IP-Adresse aufgerufen wurde, die in einer Bedrohungsliste enthalten ist. Ein Angreifer kann gestohlene Anmeldeinformationen verwenden, um diese Art der Bekanntmachung Ihrer AWS Ressourcen durchzuführen, um wertvollere Anmeldeinformationen zu finden oder die Fähigkeiten der Anmeldeinformationen zu ermitteln, die er bereits besitzt.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Recon:IAMUser/MaliciousIPCaller.Custom

Eine API wurde von einer bekannten böswilligen IP-Adresse aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie, dass ein API-Vorgang, der AWS -Ressourcen auflisten oder beschreiben kann, von einer IP-Adresse aufgerufen wurde, die in einer benutzerdefinierten Bedrohungsliste enthalten ist. Die verwendete Bedrohungsliste wird in den Ergebnisdetails aufgeführt. Ein Angreifer könnte gestohlene Anmeldeinformationen verwenden, um diese Art der Erkennung Ihrer AWS Ressourcen durchzuführen, um wertvollere Anmeldeinformationen zu finden oder die Fähigkeiten der Anmeldeinformationen zu ermitteln, die er bereits besitzt.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Recon:IAMUser/TorIPCaller

Eine API wurde von einer Tor-Exit-Knoten-IP-Adresse aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie, dass ein API-Vorgang, der Ihre AWS -Ressourcen auflisten oder beschreiben kann, von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen wurde. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Ein Angreifer würde Tor verwenden, um seine wahre Identität zu verschleiern.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail Die Protokollierung wurde deaktiviert.

Standard-Schweregrad: Niedrig

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie darüber, dass ein CloudTrail Trail in Ihrer AWS Umgebung deaktiviert wurde. Dabei kann es sich um den Versuch eines Angreifers handeln, die Protokollierung seiner Aktivitäten zu deaktivieren, indem er alle Spuren beseitigt, während er mit böswilliger Absicht Zugriff auf die AWS -Ressourcen erlangt. Dieses Ergebnis kann durch das erfolgreiche Löschen oder Aktualisieren eines Trails ausgelöst werden. Diese Erkenntnis kann auch durch das erfolgreiche Löschen eines S3-Buckets ausgelöst werden, in dem die Protokolle aus einem Trail gespeichert werden, der zugeordnet ist GuardDuty.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Stealth:IAMUser/PasswordPolicyChange

Die Passwortrichtlinie des Kontos wurde geschwächt.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Schweregrad dieser Erkenntnis kann je nach Schweregrad der an der Passwortrichtlinie vorgenommenen Änderungen Niedrig, Mittel oder Hoch sein.

- Datenquelle: CloudTrail Verwaltungsereignisse

Die AWS Kontopasswortrichtlinie wurde für das aufgeführte Konto in Ihrer AWS Umgebung geschwächt. Beispiel: Sie wurde gelöscht oder aktualisiert und erfordert jetzt weniger Zeichen, keine Sonderzeichen und Zahlen mehr, oder das Ablaufdatum des Passworts musste verlängert werden. Diese Erkenntnis kann auch durch den Versuch ausgelöst werden, Ihre AWS Kontopasswortrichtlinie zu aktualisieren oder zu löschen. Die AWS Kontopasswortrichtlinie definiert die Regeln, die regeln, welche Arten von Passwörtern für Ihre IAM-Benutzer festgelegt werden können. Eine schwächere Passwortrichtlinie ermöglicht das Erstellen von Passwörtern, die leicht zu merken und möglicherweise einfacher zu erraten sind. Dadurch entsteht ein Sicherheitsrisiko.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

Mehrere weltweit erfolgreiche Konsolenanmeldungen wurden beobachtet.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Informiert Sie darüber, dass mehrere erfolgreiche Konsolenanmeldungen für denselben IAM-Benutzer zur etwa gleichen Zeit an verschiedenen geografischen Standorten beobachtet wurden. Solche anomalen und riskanten Zugriffsstandortmuster deuten auf einen potenziellen unbefugten Zugriff auf Ihre - AWS Ressourcen hin.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

Anmeldeinformationen, die ausschließlich für eine EC2-Instance über eine Instance-Startrolle erstellt wurden, werden von einem anderen Konto innerhalb von AWSverwendet.

Standard-Schweregrad: Hoch*

> **Note**
>
> Der Standard-Schweregrad diese Erkenntnis ist Hoch. Wenn die API jedoch von einem Konto aufgerufen wurde, das Ihrer AWS Umgebung zugeordnet ist, lautet der Schweregrad Mittel.

- Datenquelle: CloudTrail Verwaltungsereignisse oder S3-Datenereignisse

Diese Erkenntnis informiert Sie darüber, wann Ihre EC2-Instance-Anmeldeinformationen verwendet werden, um APIs von einer IP-Adresse aufzurufen, die einem anderen - AWS Konto gehört als das, in dem die zugehörige EC2-Instance ausgeführt wird.

AWS empfiehlt nicht, temporäre Anmeldeinformationen außerhalb der Entität umzuverteilen, die sie erstellt hat (z. B. AWS Anwendungen, EC2 oder Lambda). Allerdings können autorisierte Benutzer Anmeldeinformationen aus EC2-Instances exportieren, um legitime API-Aufrufe durchzuführen. Wenn das `remoteAccountDetails.Affiliated` Feld ist, wurde `True` die API von einem Konto aufgerufen, das Ihrer AWS Umgebung zugeordnet ist. Um einen potenziellen Angriff auszuschließen und die Legitimität der Aktivität zu verifizieren, wenden Sie sich an den IAM-Benutzer, denen diese Anmeldeinformationen zugewiesen sind.

> **Note**
>
> Wenn die fortgesetzte Aktivität eines Remote-Kontos GuardDuty beobachtet, identifiziert sein Machine Learning (ML)-Modell dies als erwartetes Verhalten. Daher generiert dieses Ergebnis GuardDuty nicht mehr für Aktivitäten von diesem Remote-Konto. generiert GuardDuty weiterhin Ergebnisse für neues Verhalten von anderen Remote-Konten und bewertet erlernte Remote-Konten neu, wenn sich das Verhalten im Laufe der Zeit ändert.

Empfehlungen zur Abhilfe:

Als Reaktion auf diese Erkenntnis können Sie den folgenden Workflow verwenden, um eine Vorgehensweise festzulegen:

1. Identifizieren Sie das betroffene Remote-Konto im `service.action.awsApiCallAction.remoteAccountDetails.accountId`-Feld.
2. Stellen Sie als Nächstes fest, ob dieses Konto mit Ihrer GuardDuty Umgebung aus dem `service.action.awsApiCallAction.remoteAccountDetails.affiliated` Feld verknüpft ist.
3. Wenn das Konto zugeordnet ist, wenden Sie sich an den Eigentümer des Remote-Kontos und den Besitzer der EC2-Instance-Anmeldeinformationen, um dies zu überprüfen.
4. Wenn das Konto nicht zugeordnet ist, werten Sie zunächst aus, dass das Konto Ihrer Organisation zugeordnet ist, aber nicht Teil Ihrer GuardDuty Einrichtung mit mehreren Konten ist oder ob im Konto noch GuardDuty nicht aktiviert wurde. Wenden Sie sich andernfalls an den Besitzer der

EC2-Anmeldeinformationen, um festzustellen, ob es einen Anwendungsfall für die Verwendung dieser Anmeldeinformationen durch ein Remote-Konto gibt.

5. Wenn der Besitzer der Anmeldeinformationen das entfernte Konto nicht erkennt, wurden die Anmeldeinformationen möglicherweise von einem Bedrohungsakteur innerhalb von AWSkompromittiert. Sie sollten die unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance empfohlenen Maßnahmen zum Schutz Ihrer Umgebung ergreifen. Darüber hinaus können Sie einen Missbrauchsbericht an das AWS Vertrauens- und Sicherheitsteam senden, um mit einer Untersuchung des Remote-Kontos zu beginnen. Wenn Sie Ihre Meldung an AWS Trust and Safety einreichen, geben Sie bitte die vollständigen JSON-Details der Erkenntnis an.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Anmeldeinformationen, die über eine Instance-Startrolle ausschließlich für eine EC2-Instance erstellt wurden, werden von einer externen IP-Adresse verwendet.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Verwaltungsereignisse oder S3-Datenereignisse

Diese Erkenntnis informiert Sie darüber, dass ein Host außerhalb von versucht AWS hat, AWS API-Operationen mit temporären AWS Anmeldeinformationen auszuführen, die auf einer EC2-Instance in Ihrer AWS Umgebung erstellt wurden. Die aufgeführte EC2-Instance ist möglicherweise kompromittiert, und die temporären Anmeldeinformationen von dieser Instance wurden möglicherweise auf einen Remote-Host außerhalb von AWS herausgefiltert AWS. empfiehlt nicht, temporäre Anmeldeinformationen außerhalb der Entität neu zu verteilen, die sie erstellt hat (z. B. AWS Anwendungen, EC2 oder Lambda). Allerdings können autorisierte Benutzer Anmeldeinformationen aus EC2-Instances exportieren, um legitime API-Aufrufe durchzuführen. Um einen potenziellen Angriff auszuschließen und die Legitimität der Aktivität zu überprüfen, überprüfen Sie, ob die Verwendung von Instance-Anmeldeinformationen von der Remote-IP in der Erkenntnis erwartet wird.

> **Note**
>
> Wenn die fortgesetzte Aktivität eines Remote-Kontos GuardDuty beobachtet, identifiziert sein Machine Learning (ML)-Modell dies als erwartetes Verhalten. Daher generiert dieses Ergebnis GuardDuty nicht mehr für Aktivitäten von diesem Remote-Konto. generiert

GuardDuty weiterhin Ergebnisse für neues Verhalten von anderen Remote-Konten und bewertet erlernte Remote-Konten neu, wenn sich das Verhalten im Laufe der Zeit ändert.

Empfehlungen zur Abhilfe:

Diese Erkenntnis wird generiert, wenn das Netzwerk so konfiguriert ist, dass der Internetverkehr von einem On-Premises-Gateway und nicht von einem VPC Internet Gateway (IGW) ausgeht. Geläufige Konfigurationen, z. B. die Verwendung von AWS Outposts, oder VPC-VPN-Verbindungen, können dazu führen, dass Datenverkehr auf diese Weise weitergeleitet wird. Wenn dies ein erwartetes Verhalten ist, empfiehlt es sich, Unterdrückungsregeln zu verwenden und eine Regel zu erstellen, die aus zwei Filterkriterien besteht. Das erste Kriterium ist der Ergebnistyp, der `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS` sein sollte. Das zweite Filterkriterium ist die IPv4-Adresse des API-Aufrufers mit der IP-Adresse oder dem CIDR-Bereich Ihres On-Premises-Internet-Gateways. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

> **Note**
>
> Wenn die kontinuierliche Aktivität aus einer externen Quelle GuardDuty beobachtet, identifiziert sein Machine-Learning-Modell dies als erwartetes Verhalten und generiert dieses Ergebnis nicht mehr für Aktivitäten aus dieser Quelle. generiert GuardDuty weiterhin Ergebnisse für neues Verhalten aus anderen Quellen und bewertet erlernte Quellen neu, wenn sich das Verhalten im Laufe der Zeit ändert.

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

UnauthorizedAccess:IAMUser/MaliciousIPCaller

Eine API wurde von einer bekannten böswilligen IP-Adresse aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie darüber, dass eine API-Operation (z. B. ein Versuch, eine EC2-Instance zu starten, einen neuen IAM-Benutzer zu erstellen oder Ihre AWS Berechtigungen zu ändern) von einer bekannten bösartigen IP-Adresse aus aufgerufen wurde. Dies kann auf unbefugten Zugriff auf AWS Ressourcen in Ihrer Umgebung hinweisen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

Eine API wurde von einer IP-Adresse aufgerufen, die sich auf einer benutzerdefinierten Bedrohungsliste befindet.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie darüber, dass eine API-Operation (z. B. ein Versuch, eine EC2-Instance zu starten, einen neuen IAM-Benutzer zu erstellen oder AWS Berechtigungen zu ändern) von einer IP-Adresse aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. In besteht eine Bedrohungsliste aus bekannten schädlichen IP-Adressen. Dies kann auf unbefugten Zugriff auf AWS Ressourcen in Ihrer Umgebung hinweisen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

UnauthorizedAccess:IAMUser/TorIPCaller

Eine API wurde von einer Tor-Exit-Knoten-IP-Adresse aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang (Beispiel: ein Versuch zum Starten einer EC2-Instance, Erstellen eines neuen IAM-Benutzers oder Ändern Ihrer AWS -Rechte) von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen wurde. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf Ihre AWS -Ressourcen hinweisen, mit dem Ziel, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

EKS-Auditprotokolle, Typen finden

Die folgenden Erkenntnisse beziehen sich auf Kubernetes-Ressourcen und haben einen resource_type `EKSCluster`. Der Schweregrad und die Details der Erkenntnisse unterscheiden sich je nach Erkenntnistyp.

Für alle Erkenntnisse des Kubernetes-Typs empfehlen wir, dass Sie die betreffende Ressource untersuchen, um festzustellen, ob es sich um eine erwartete oder potenziell bösartige Aktivität handelt. Hinweise zur Behebung einer gefährdeten Kubernetes-Ressource, die durch einen Befund identifiziert wurde, finden Sie unter. GuardDuty Behebung der Erkenntnisse von EKS Audit Log Monitoring

> **Note**
>
> Wenn die Aktivität, aufgrund derer diese Erkenntnisse generiert werden, erwartet wird, sollten Sie erwägen, Unterdrückungsregeln sie hinzuzufügen, um zukünftige Benachrichtigungen zu verhindern.

Themen

- CredentialAccess:Kubernetes/MaliciousIPCaller
- CredentialAccess:Kubernetes/MaliciousIPCaller.Custom
- CredentialAccess:Kubernetes/SuccessfulAnonymousAccess
- CredentialAccess:Kubernetes/TorIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller

- DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom
- DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess
- DefenseEvasion:Kubernetes/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller
- Discovery:Kubernetes/MaliciousIPCaller.Custom
- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Impact:Kubernetes/SuccessfulAnonymousAccess
- Impact:Kubernetes/TorIPCaller
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Persistence:Kubernetes/MaliciousIPCaller
- Persistence:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/SuccessfulAnonymousAccess
- Persistence:Kubernetes/TorIPCaller
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/KubeflowDashboardExposed
- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

> **Note**
>
> Vor Kubernetes Version 1.14 war die `system:unauthenticated` Gruppe standardmäßig mit und verknüpft. `system:discovery` `system:basic-user` ClusterRoles Diese Zuordnung kann unbeabsichtigten Zugriff durch anonyme Benutzer ermöglichen. Durch Cluster-Updates werden diese Berechtigungen nicht aufgehoben. Auch wenn Sie Ihren Cluster auf Version 1.14 oder höher aktualisiert haben, sind diese Berechtigungen möglicherweise weiterhin aktiviert. Wir empfehlen, dass Sie die Zuordnung dieser Berechtigungen zu der `system:unauthenticated`-Gruppe aufheben. Anleitungen zum Widerrufen dieser Berechtigungen finden Sie unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch.

CredentialAccess:Kubernetes/MaliciousIPCaller

Eine API, die häufig für den Zugriff auf Anmeldeinformationen oder Geheimnisse in einem Kubernetes-Cluster verwendet wird, wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit der Phase des Zugriffs auf Anmeldeinformationen in Verbindung gebracht, wenn ein Angreifer versucht, Passwörter, Benutzernamen und Zugriffsschlüssel für Ihren Kubernetes-Cluster zu sammeln.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen und gegebenenfalls die Berechtigungen widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine

böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

Eine API, die häufig für den Zugriff auf Anmeldeinformationen oder Geheimnisse in einem Kubernetes-Cluster verwendet wird, wurde von einer IP-Adresse auf einer benutzerdefinierten Bedrohungsliste aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Die beobachtete API wird häufig mit der Taktik des Zugriffs auf Anmeldeinformationen in Verbindung gebracht, wenn ein Angreifer versucht, Passwörter, Benutzernamen und Zugriffsschlüssel für Ihren Kubernetes-Cluster zu sammeln.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte, und widerrufen Sie gegebenenfalls die Berechtigungen, indem Sie die Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

Eine API, die häufig für den Zugriff auf Anmeldeinformationen oder Geheimnisse in einem Kubernetes-Cluster verwendet wird, wurde von einem nicht authentifizierten Benutzer aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang vom `system:anonymous`-Benutzer erfolgreich aufgerufen wurde. API-Aufrufe von `system:anonymous` sind nicht authentifiziert. Die beobachtete API wird häufig mit der Taktik des Zugriffs auf Anmeldeinformationen in Verbindung gebracht, wenn ein Angreifer versucht, Passwörter, Benutzernamen und Zugriffsschlüssel für Ihren Kubernetes-Cluster zu sammeln. Diese Aktivität weist darauf hin, dass anonymer oder nicht authentifizierter Zugriff auf die in der Erkenntnis gemeldete API-Aktion zulässig ist und bei anderen Aktionen möglicherweise zulässig ist. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch.

Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

CredentialAccess:Kubernetes/TorIPCaller

Eine API, die häufig für den Zugriff auf Anmeldeinformationen oder Geheimnisse in einem Kubernetes-Cluster verwendet wird, wurde von einer bekannten bösartigen Tor-Ausgangsknotens-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Die Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen wurde. Die beobachtete API wird häufig mit der Taktik des Zugriffs

auf Anmeldeinformationen in Verbindung gebracht, wenn ein Angreifer versucht, Passwörter, Benutzernamen und Zugriffsschlüssel für Ihren Kubernetes-Cluster zu sammeln. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf die Kubernetes-Cluster-Ressourcen hinweisen, mit dem Ziel, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen und gegebenenfalls die Berechtigungen widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

DefenseEvasion:Kubernetes/MaliciousIPCaller

Eine API, die häufig verwendet wird, um Abwehrmaßnahmen zu umgehen, wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit Umgehungstaktiken in Verbindung gebracht, bei denen ein Gegner versucht, seine Aktionen zu verbergen, um nicht entdeckt zu werden.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen und gegebenenfalls die Berechtigungen widerrufen durfte. Folgen Sie

dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

Eine API, die üblicherweise zur Umgehung von Abwehrmaßnahmen verwendet wird, wurde von einer IP-Adresse auf einer benutzerdefinierten Bedrohungsliste aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Die beobachtete API wird häufig mit Umgehungstaktiken in Verbindung gebracht, bei denen ein Gegner versucht, seine Aktionen zu verbergen, um nicht entdeckt zu werden.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen und gegebenenfalls die Berechtigungen widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

Eine API, die häufig verwendet wird, um Abwehrmaßnahmen zu umgehen, wurde von einem nicht authentifizierten Benutzer aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang vom `system:anonymous`-Benutzer erfolgreich aufgerufen wurde. API-Aufrufe von `system:anonymous` sind nicht authentifiziert. Die beobachtete API wird häufig mit Taktiken zur Umgehung der Verteidigung in Verbindung gebracht, bei der ein Gegner versucht, seine Aktionen zu verbergen, um nicht entdeckt zu werden. Diese Aktivität weist darauf hin, dass anonymer oder nicht authentifizierter Zugriff auf die in der Erkenntnis gemeldete API-Aktion zulässig ist und bei anderen Aktionen möglicherweise zulässig ist. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch.

Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

DefenseEvasion:Kubernetes/TorIPCaller

Eine API, die häufig verwendet wird, um Abwehrmaßnahmen zu umgehen, wurde von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Die Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen wurde. Die beobachtete API wird häufig mit Umgehungstaktiken in Verbindung gebracht, bei denen ein Gegner versucht, seine Aktionen zu verbergen, um nicht entdeckt zu werden. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und

leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf Ihren Kubernetes-Cluster hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen und gegebenenfalls die Berechtigungen widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Discovery:Kubernetes/MaliciousIPCaller

Eine API, die häufig zur Erkennung von Ressourcen in einem Kubernetes-Cluster verwendet wird, wurde von einer IP-Adresse aus aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig in der Erkennungsphase eines Angriffs verwendet, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihr Kubernetes-Cluster für einen umfassenderen Angriff anfällig ist.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen und gegebenenfalls die Berechtigungen widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine

böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Discovery:Kubernetes/MaliciousIPCaller.Custom

Eine API, die häufig zur Erkennung von Ressourcen in einem Kubernetes-Cluster verwendet wird, wurde von einer IP-Adresse aus einer benutzerdefinierten Bedrohungsliste aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass eine API von einer IP-Adresse aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Die beobachtete API wird häufig in der Erkennungsphase eines Angriffs verwendet, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihr Kubernetes-Cluster für einen umfassenderen Angriff anfällig ist.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen und gegebenenfalls die Berechtigungen widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Discovery:Kubernetes/SuccessfulAnonymousAccess

Eine API, die häufig zur Erkennung von Ressourcen in einem Kubernetes-Cluster verwendet wird, wurde von einem nicht authentifizierten Benutzer aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang vom `system:anonymous`-Benutzer erfolgreich aufgerufen wurde. API-Aufrufe von `system:anonymous` sind nicht authentifiziert. Die beobachtete API wird häufig mit der Erkennungsphase eines Angriffs in Verbindung gebracht, in der ein Angreifer Informationen über Ihren Kubernetes-Cluster sammelt. Diese Aktivität weist darauf hin, dass anonymer oder nicht authentifizierter Zugriff auf die in der Erkenntnis gemeldete API-Aktion zulässig ist und bei anderen Aktionen möglicherweise zulässig ist. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch.

Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Discovery:Kubernetes/TorIPCaller

Eine API, die häufig zur Erkennung von Ressourcen in einem Kubernetes-Cluster verwendet wird, wurde von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Die Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen wurde. Die beobachtete API wird häufig in der Erkennungsphase eines Angriffs verwendet, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihr Kubernetes-Cluster

für einen umfassenderen Angriff anfällig ist. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf Ihren Kubernetes-Cluster hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen durfte, und widerrufen Sie gegebenenfalls die Berechtigungen, indem Sie die Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Execution:Kubernetes/ExecInKubeSystemPod

Ein Befehl wurde in einem Pod innerhalb des **`kube-system`**-Namespace ausgeführt

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Befehl in einem Pod innerhalb des `kube-system`-Namespace mithilfe der Kubernetes-Exec-API ausgeführt wurde. `kube-system`-Namespace ist ein Standard-Namespaces, der hauptsächlich für Komponenten auf Systemebene wie `kube-dns` und `kube-proxy` verwendet wird. Es ist sehr ungewöhnlich, Befehle innerhalb von Pods oder Containern unter einem `kube-system`-Namespace auszuführen, was auf verdächtige Aktivitäten hinweisen kann.

Empfehlungen zur Abhilfe:

Wenn die Ausführung dieses Befehls unerwartet erfolgt, können die Anmeldeinformationen der Benutzeridentität, die zur Ausführung des Befehls verwendet wurde, kompromittiert sein. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer

an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Impact:Kubernetes/MaliciousIPCaller

Eine API, die häufig zur Manipulation von Ressourcen in einem Kubernetes-Cluster verwendet wird, wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit Schlagtaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten in Ihrer Umgebung zu manipulieren, zu unterbrechen oder zu zerstören. AWS

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen und gegebenenfalls die Berechtigungen widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Impact:Kubernetes/MaliciousIPCaller.Custom

Eine API, die häufig zur Manipulation von Ressourcen in einem Kubernetes-Cluster verwendet wird, wurde von einer IP-Adresse auf einer benutzerdefinierten Bedrohungsliste aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Die beobachtete API wird häufig mit Schlagtaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten in Ihrer Umgebung zu manipulieren, zu unterbrechen oder zu zerstören. AWS

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen und gegebenenfalls die Berechtigungen widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Impact:Kubernetes/SuccessfulAnonymousAccess

Eine API, die häufig zur Manipulation von Ressourcen in einem Kubernetes-Cluster verwendet wird, wurde von einem nicht authentifizierten Benutzer aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang vom `system:anonymous`-Benutzer erfolgreich aufgerufen wurde. API-Aufrufe von `system:anonymous` sind nicht authentifiziert. Die beobachtete API wird häufig mit der Auswirkungsphase eines Angriffs in Verbindung gebracht, wenn ein Angreifer Ressourcen in Ihrem Cluster manipuliert. Diese Aktivität weist darauf hin, dass anonymer oder nicht authentifizierter Zugriff auf die in der Erkenntnis gemeldete API-Aktion zulässig ist und bei anderen Aktionen möglicherweise zulässig ist. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch.

Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Impact:Kubernetes/TorIPCaller

Eine API, die häufig verwendet wird, um Ressourcen in einem Kubernetes-Cluster zu manipulieren, wurde von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Die Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen wurde. Die beobachtete API wird häufig mit Auswirkungstaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten in Ihrer AWS -Umgebung zu manipulieren, zu unterbrechen oder zu zerstören. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf Ihren Kubernetes-Cluster hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen und gegebenenfalls die Berechtigungen widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen

rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Persistence:Kubernetes/ContainerWithSensitiveMount

Ein Container wurde gestartet, in dem ein sensibler externer Host-Pfad eingehängt war.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Container mit einer Konfiguration gestartet wurde, die im Abschnitt `volumeMounts` einen sensiblen Host-Pfad mit Schreibzugriff enthielt. Dadurch ist der sensible Host-Pfad vom Container aus zugänglich und beschreibbar. Diese Technik wird häufig von Gegnern verwendet, um Zugriff auf das Dateisystem des Hosts zu erhalten.

Empfehlungen zur Abhilfe:

Wenn dieser Container-Start unerwartet erfolgt, können die Anmeldeinformationen der Benutzeridentität, die zum Starten des Containers verwendet wurde, kompromittiert sein. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Wenn dieser Container-Start erwartet wird, wird empfohlen, eine Unterdrückungsregel zu verwenden, die aus Filterkriterien besteht, die auf dem Feld `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` basieren. In den Filterkriterien sollte das `imagePrefix`-Feld dem in der Erkenntnis angegebenen Feld `imagePrefix` entsprechen. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Persistence:Kubernetes/MaliciousIPCaller

Eine API, die üblicherweise verwendet wird, um dauerhaften Zugriff auf einen Kubernetes-Cluster zu erhalten, wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit Persistenz-Taktiken in Verbindung gebracht, bei denen sich ein Angreifer Zugriff auf Ihren Kubernetes-Cluster verschafft hat und versucht, diesen Zugriff aufrechtzuerhalten.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen und gegebenenfalls die Berechtigungen widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Persistence:Kubernetes/MaliciousIPCaller.Custom

Eine API, die häufig verwendet wird, um dauerhaften Zugriff auf einen Kubernetes-Cluster zu erhalten, wurde von einer IP-Adresse aus einer benutzerdefinierten Bedrohungsliste aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Die beobachtete API wird häufig mit Persistenz-Taktiken in Verbindung gebracht, bei denen sich ein Angreifer Zugriff auf Ihren Kubernetes-Cluster verschafft hat und versucht, diesen Zugriff aufrechtzuerhalten.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen und gegebenenfalls die Berechtigungen widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Persistence:Kubernetes/SuccessfulAnonymousAccess

Eine API, die häufig verwendet wird, um hochgradige Berechtigungen für einen Kubernetes-Cluster zu erhalten, wurde von einem nicht authentifizierten Benutzer aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein API-Vorgang vom `system:anonymous`-Benutzer erfolgreich aufgerufen wurde. API-Aufrufe von `system:anonymous` sind nicht authentifiziert. Die beobachtete API wird häufig mit Persistenztaktiken in Verbindung gebracht, bei denen sich ein Angreifer Zugriff auf Ihren Cluster verschafft hat und versucht, diesen Zugriff aufrechtzuerhalten. Diese Aktivität weist darauf hin, dass anonymer oder nicht authentifizierter Zugriff auf die in der Erkenntnis gemeldete API-Aktion zulässig ist und bei anderen Aktionen möglicherweise zulässig ist. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch.

Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Persistence:Kubernetes/TorIPCaller

Eine API, die häufig verwendet wird, um dauerhaften Zugriff auf einen Kubernetes-Cluster zu erhalten, wurde von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Die Erkenntnis informiert Sie darüber, dass ein API-Vorgang von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen wurde. Die beobachtete API wird häufig mit Persistenz-Taktiken in Verbindung gebracht, bei denen sich ein Angreifer Zugriff auf Ihren Kubernetes-Cluster verschafft hat und versucht, diesen Zugriff aufrechtzuerhalten. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf Ihre AWS Ressourcen hinweisen, mit der Absicht, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API aufrufen und gegebenenfalls die Berechtigungen widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

Dem Standard-Servicekonto wurden Administratorrechte auf einem Kubernetes-Cluster gewährt.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass dem Standard-Servicekonto für einen Namespace in Ihrem Kubernetes-Cluster Administratorrechte gewährt wurden. Kubernetes erstellt ein Standard-Servicekonto für alle Namespaces im Cluster. Es weist Pods, die nicht explizit einem anderen Servicekonto zugeordnet wurden, automatisch das Standard-Servicekonto als Identität zu. Wenn das Standard-Servicekonto über Administratorrechte verfügt, kann dies dazu führen, dass Pods unbeabsichtigt mit Administratorrechten gestartet werden. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten nicht das Standard-Servicekonto verwenden, um Pods Berechtigungen zu erteilen. Stattdessen sollten Sie für jeden Workload ein eigenes Servicekonto erstellen und diesem Konto je nach Bedarf Berechtigungen erteilen. Um dieses Problem zu beheben, sollten Sie spezielle Servicekonten für all Ihre Pods und Workloads erstellen und die Pods und Workloads aktualisieren, um vom Standard-Servicekonto zu ihren dedizierten Konten zu migrieren. Anschließend sollten Sie die Administratorberechtigung aus dem Standard-Servicekonto entfernen. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Policy:Kubernetes/AnonymousAccessGranted

Dem **`system:anonymous`**-Benutzer wurde die API-Berechtigung für einen Kubernetes-Cluster erteilt.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Benutzer in Ihrem Kubernetes-Cluster erfolgreich ein `ClusterRoleBinding` oder `RoleBinding` erstellt hat, um den Benutzer `system:anonymous` an eine Rolle zu binden. Dies ermöglicht einen nicht authentifizierten Zugriff auf die API-Vorgänge, die von der Rolle zugelassen werden. Wenn dieses Verhalten nicht erwartet wird, deutet dies

möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer oder der `system:unauthenticated`-Gruppe in Ihrem Cluster gewährt wurden, und unnötigen anonymen Zugriff widerrufen. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon EKS im Amazon EKS-Benutzerhandbuch. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Policy:Kubernetes/ExposedDashboard

Das Dashboard für einen Kubernetes-Cluster war im Internet verfügbar

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass das Kubernetes-Dashboard für Ihren Cluster über einen Load Balancer-Service dem Internet zugänglich gemacht wurde. Ein offengelegtes Dashboard ermöglicht den Zugriff auf die Verwaltungsoberfläche Ihres Clusters über das Internet und ermöglicht es Gegnern, eventuell vorhandene Lücken in der Authentifizierungs- und Zugriffssteuerung auszunutzen.

Empfehlungen zur Abhilfe:

Sie sollten sicherstellen, dass im Kubernetes-Dashboard eine starke Authentifizierung und Autorisierung durchgesetzt wird. Sie sollten auch eine Netzwerk-Zugriffssteuerung implementieren, um den Zugriff auf das Dashboard von bestimmten IP-Adressen aus zu beschränken.

Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Policy:Kubernetes/KubeflowDashboardExposed

Das Kubeflow-Dashboard für einen Kubernetes-Cluster war im Internet verfügbar

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass das Kubeflow-Dashboard für Ihren Cluster über einen Load Balancer-Service dem Internet zugänglich gemacht wurde. Ein offengelegtes Kubeflow-Dashboard ermöglicht den Zugriff auf die Verwaltungsoberfläche Ihrer Kubeflow-Umgebung über das Internet und ermöglicht es Gegnern, eventuell vorhandene Lücken in der Authentifizierung und Zugriffssteuerung auszunutzen.

Empfehlungen zur Abhilfe:

Sie sollten sicherstellen, dass im Kubeflow-Dashboard eine starke Authentifizierung und Autorisierung durchgesetzt wird. Sie sollten auch eine Netzwerk-Zugriffssteuerung implementieren, um den Zugriff auf das Dashboard von bestimmten IP-Adressen aus zu beschränken.

Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

PrivilegeEscalation:Kubernetes/PrivilegedContainer

Ein privilegierter Container mit Zugriff auf Root-Ebene wurde auf Ihrem Kubernetes-Cluster gestartet.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein privilegierter Container, der auf Ihrem Kubernetes-Cluster mithilfe eines Images gestartet wurde, das noch nie zuvor verwendet wurde, um privilegierte Container in Ihrem Cluster zu starten. Ein privilegierter Container hat Zugriff auf Root-Ebene auf den Host. Angreifer können als Taktik zur Erweiterung ihrer Rechte privilegierte Container starten, um sich Zugriff auf den Host zu verschaffen und ihn dann zu kompromittieren.

Empfehlungen zur Abhilfe:

Wenn dieser Container-Start unerwartet erfolgt, können die Anmeldeinformationen der Benutzeridentität, die zum Starten des Containers verwendet wurde, kompromittiert sein. Sperren

Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

Eine Kubernetes-API, die häufig für den Zugriff auf Geheimnisse verwendet wird, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Kubernetes-Benutzer in Ihrem Cluster einen anomalen API-Vorgang zum Abrufen vertraulicher Cluster-Geheimnisse aufgerufen hat. Die beobachtete API wird häufig mit Taktiken für den Zugriff auf Anmeldeinformationen in Verbindung gebracht, die zu einer privilegierten Eskalation und weiterem Zugriff innerhalb Ihres Clusters führen können. Wenn dieses Verhalten nicht erwartet wird, kann dies entweder auf einen Konfigurationsfehler hinweisen oder darauf, dass Ihre AWS Anmeldeinformationen kompromittiert wurden.

Die beobachtete API wurde durch das Modell des maschinellen Lernens (ML) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer-API-Aktivitäten innerhalb Ihres EKS-Clusters und identifiziert anomale Ereignisse, die mit Techniken in Verbindung stehen, die von nicht autorisierten Benutzern verwendet werden. Das ML-Modell verfolgt mehrere Faktoren des API-Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API-Anfrage finden Sie im Bereich mit den Suchdetails in der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem Kubernetes-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass all diese Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Falls Ihre AWS Anmeldedaten kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell gefährdeter Anmeldeinformationen AWS.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

In Ihrem RoleBinding ClusterRoleBinding Kubernetes-Cluster wurde ein oder für eine übermäßig freizügige Rolle oder einen sensiblen Namespace erstellt oder geändert.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn ein RoleBinding oder jedoch das Oder ClusterRoleBinding beinhaltet, ist der Schweregrad Hoch ClusterRoles `admin`. `cluster-admin`

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Benutzer in Ihrem Kubernetes-Cluster ein `RoleBinding` oder `ClusterRoleBinding` erstellt hat, um einen Benutzer an eine Rolle mit Administratorberechtigungen oder sensiblen Namespaces zu binden. Wenn dieses Verhalten nicht erwartet wird, kann dies entweder auf einen Konfigurationsfehler hinweisen oder darauf, dass Ihre AWS Anmeldeinformationen kompromittiert wurden.

Die beobachtete API wurde durch das Modell des maschinellen Lernens (ML) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer-API-Aktivitäten innerhalb Ihres EKS-Clusters. Dieses ML-Modell identifiziert auch ungewöhnliche Ereignisse, die mit den von einem nicht autorisierten Benutzer verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt mehrere Faktoren des API-Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API-Anfrage finden Sie im Bereich mit den Suchdetails in der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Untersuchen Sie die dem Kubernetes-Benutzer erteilten Berechtigungen. Diese Berechtigungen sind in der Rolle und den beteiligten Subjekten in `RoleBinding` und `ClusterRoleBinding`

definiert. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Falls Ihre AWS Anmeldedaten kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell gefährdeter Anmeldeinformationen AWS.

Execution:Kubernetes/AnomalousBehavior.ExecInPod

Ein Befehl wurde in einem Pod auf ungewöhnliche Weise ausgeführt.

Standard-Schweregrad: Mittel

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Befehl in einem Pod mithilfe der Kubernetes-Exec-API ausgeführt wurde. Die Kubernetes-Exec-API ermöglicht die Ausführung beliebiger Befehle in einem Pod. Wenn dieses Verhalten für den Benutzer, den Namespace oder den Pod nicht erwartet wird, kann dies entweder auf einen Konfigurationsfehler hinweisen oder darauf, dass Ihre AWS Anmeldeinformationen kompromittiert wurden.

Die beobachtete API wurde durch das ML-Modell (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer-API-Aktivitäten innerhalb Ihres EKS-Clusters. Dieses ML-Modell identifiziert auch ungewöhnliche Ereignisse, die mit den von einem nicht autorisierten Benutzer verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt mehrere Faktoren des API-Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API-Anfrage finden Sie im Bereich mit den Suchdetails in der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn die Ausführung dieses Befehls unerwartet erfolgt, wurden möglicherweise die Anmeldeinformationen der Benutzeridentität, die zur Ausführung des Befehls verwendet wurde, kompromittiert. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Falls Ihre AWS Anmeldedaten kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell gefährdeter Anmeldeinformationen AWS.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

Ein Workload wurde mit einem privilegierten Container auf ungewöhnliche Weise gestartet.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Workload mit einem privilegierten Container in Ihrem Amazon-EKS-Cluster gestartet wurde. Ein privilegierter Container hat Zugriff auf Root-Ebene auf den Host. Unbefugte Benutzer können privilegierte Container als Taktik zur Rechteerweiterung starten, um sich zunächst Zugriff auf den Host zu verschaffen und ihn dann zu kompromittieren.

Die beobachtete Erstellung oder Änderung eines Containers wurde anhand des ML-Modells (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer-API- und Container-Image-Aktivitäten innerhalb Ihres EKS-Clusters. Dieses ML-Modell identifiziert auch ungewöhnliche Ereignisse, die mit den von einem nicht autorisierten Benutzer verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt mehrere Faktoren des API-Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten, in Ihrem Konto beobachtete Container-Images und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API-Anfrage finden Sie im Bereich mit den Suchdetails in der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn dieser Container-Start unerwartet erfolgt, wurden möglicherweise die Anmeldeinformationen der Benutzeridentität, die zum Starten des Containers verwendet wurde, kompromittiert. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Falls Ihre AWS Anmeldedaten kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell gefährdeter Anmeldeinformationen AWS.

Wenn dieser Container-Start erwartet wird, empfiehlt es sich, eine Unterdrückungsregel mit Filterkriterien zu verwenden, die auf dem `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`-Feld basieren. In den Filterkriterien sollte das `imagePrefix`-Feld dem in der Erkenntnis angegebenen Feld `imagePrefix` entsprechen. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount

Ein Workload wurde auf ungewöhnliche Weise bereitgestellt, wobei ein sensibler Host-Pfad innerhalb des Workloads eingehängt wurde.

Standard-Schweregrad: Hoch

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Workload mit einem Container gestartet wurde, der im Abschnitt `volumeMounts` einen sensiblen Host-Pfad enthielt. Dadurch ist der sensible Host-Pfad potenziell vom Container aus zugänglich und beschreibbar. Diese Technik wird häufig von Gegnern verwendet, um Zugriff auf das Dateisystem des Hosts zu erhalten.

Die beobachtete Erstellung oder Änderung eines Containers wurde anhand des ML-Modells (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer-API- und Container-Image-Aktivitäten innerhalb Ihres EKS-Clusters. Dieses ML-Modell identifiziert auch ungewöhnliche Ereignisse, die mit den von einem nicht autorisierten Benutzer verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt mehrere Faktoren des API-Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten, in Ihrem Konto beobachtete Container-Images und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API-Anfrage finden Sie im Bereich mit den Suchdetails in der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn dieser Container-Start unerwartet erfolgt, wurden möglicherweise die Anmeldeinformationen der Benutzeridentität, die zum Starten des Containers verwendet wurde, kompromittiert. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer

an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Falls Ihre AWS Anmeldedaten kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell gefährdeter Anmeldeinformationen AWS.

Wenn dieser Container-Start erwartet wird, empfiehlt es sich, eine Unterdrückungsregel mit Filterkriterien zu verwenden, die auf dem `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`-Feld basieren. In den Filterkriterien sollte das `imagePrefix`-Feld dem in der Erkenntnis angegebenen Feld `imagePrefix` entsprechen. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

Ein Workload wurde auf ungewöhnliche Weise gestartet.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Standardschweregrad ist Niedrig. Wenn der Workload jedoch einen potenziell verdächtigen Image-Namen enthält, z. B. ein bekanntes Pentest-Tool, oder einen Container, in dem beim Start ein potenziell verdächtiger Befehl ausgeführt wird, z. B. Reverse-Shell-Befehle, wird der Schweregrad dieses Ergebnistyps als Mittel eingestuft.

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Kubernetes-Workload in Ihrem Amazon EKS-Cluster auf ungewöhnliche Weise erstellt oder geändert wurde, z. B. durch eine API-Aktivität, neue Container-Images oder eine riskante Workload-Konfiguration. Unbefugte Benutzer können privilegierte Container als Taktik zur Rechteerweiterung starten, um sich zunächst Zugriff auf den Host zu verschaffen und ihn dann zu kompromittieren.

Die beobachtete Erstellung oder Änderung eines Containers wurde anhand des ML-Modells (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer-API- und Container-Image-Aktivitäten innerhalb Ihres EKS-Clusters. Dieses

ML-Modell identifiziert auch ungewöhnliche Ereignisse, die mit den von einem nicht autorisierten Benutzer verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt mehrere Faktoren des API-Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten, in Ihrem Konto beobachtete Container-Images und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API-Anfrage finden Sie im Bereich mit den Suchdetails in der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn dieser Container-Start unerwartet erfolgt, wurden möglicherweise die Anmeldeinformationen der Benutzeridentität, die zum Starten des Containers verwendet wurde, kompromittiert. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Falls Ihre AWS Anmeldedaten kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell gefährdeter Anmeldeinformationen AWS.

Wenn dieser Container-Start erwartet wird, empfiehlt es sich, eine Unterdrückungsregel mit Filterkriterien zu verwenden, die auf dem `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`-Feld basieren. In den Filterkriterien sollte das `imagePrefix`-Feld dem in der Erkenntnis angegebenen Feld `imagePrefix` entsprechen. Weitere Informationen finden Sie unter Unterdrückungsregeln.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Eine sehr freizügige Rolle oder ClusterRole wurde auf ungewöhnliche Weise erstellt oder geändert.

Standard-Schweregrad: Niedrig

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Kubernetes-Benutzer in Ihrem Amazon-EKS-Cluster einen anomale API-Vorgang zur Erstellung eines `Role` oder `ClusterRole` mit übermäßigen Berechtigungen aufgerufen hat. Akteure können die Rollenerstellung mit leistungsstarken Berechtigungen verwenden, um die Verwendung integrierter Administratorrollen zu vermeiden

und so zu verhindern, dass sie entdeckt werden. Die übermäßigen Berechtigungen können zur Eskalation von Rechten, zur Ausführung von Remote-Code und möglicherweise zur Kontrolle über einen Namespace oder Cluster führen. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre -Anmeldeinformationen kompromittiert wurden.

Die beobachtete API wurde anhand des ML-Modells (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer-API-Aktivitäten innerhalb Ihres Amazon-EKS-Clusters und identifiziert anomale Ereignisse, die mit Techniken in Verbindung stehen, die von nicht autorisierten Benutzern verwendet werden. Das ML-Modell verfolgt mehrere Faktoren des API-Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten, in Ihrem Konto beobachtete Container-Images und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API-Anfrage finden Sie im Bereich mit den Suchdetails in der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Prüfen Sie die in `Role` oder `ClusterRole` definierten Berechtigungen, um sicherzustellen, dass alle Berechtigungen benötigt werden, und halten Sie sich an die Grundsätze der geringsten Berechtigung. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Falls Ihre AWS Anmeldedaten kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell gefährdeter Anmeldeinformationen AWS.

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Ein Benutzer hat seine Zugriffsberechtigungen auf ungewöhnliche Weise überprüft.

Standard-Schweregrad: Niedrig

- Funktion: EKS-Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Benutzer in Ihrem Kubernetes-Cluster erfolgreich geprüft hat, ob die bekannten mächtigen Berechtigungen, die zu privilegierter Eskalation und Remote-Codeausführung führen können, zulässig sind. Ein gängiger Befehl, der verwendet wird,

um die Berechtigungen eines Benutzers zu überprüfen, ist beispielsweise `kubectl auth can-i`. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Die beobachtete API wurde anhand des ML-Modells (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer-API-Aktivitäten innerhalb Ihres Amazon-EKS-Clusters und identifiziert anomale Ereignisse, die mit Techniken in Verbindung stehen, die von nicht autorisierten Benutzern verwendet werden. Das ML-Modell verfolgt auch mehrere Faktoren des API-Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, die Überprüfung der Berechtigungen und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API-Anfrage finden Sie im Bereich mit den Suchdetails in der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Prüfen Sie die dem Kubernetes-Benutzer erteilten Berechtigungen, um sicherzustellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Falls Ihre AWS Anmeldedaten kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell gefährdeter Anmeldeinformationen AWS.

Lambda-Protection-Erkenntnistypen

In diesem Abschnitt werden die Erkenntnistypen beschrieben, die für Ihre AWS Lambda-Ressourcen spezifisch sind und in denen die `resourceType` als `Lambda` aufgeführt sind. Für alle Lambda-Erkenntnisse wird empfohlen, die betreffende Ressource zu untersuchen, um festzustellen, ob sie sich erwartungsgemäß verhält. Wenn die Aktivität autorisiert ist, können Sie Unterdrückungsregeln oder Listen vertrauenswürdiger IP-Adressen und Bedrohungen verwenden, um Falschmeldungen für diese Ressource zu verhindern.

Wenn die Aktivität unerwartet ist, besteht die bewährte Sicherheitsmethode darin, davon auszugehen, dass Lambda potenziell kompromittiert wurde, und die Empfehlungen zur Behebung zu befolgen.

Themen

- Backdoor:Lambda/C&CActivity.B
- CryptoCurrency:Lambda/BitcoinTool.B

- Trojan:Lambda/BlackholeTraffic
- Trojan:Lambda/DropPoint
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- UnauthorizedAccess:Lambda/TorClient
- UnauthorizedAccess:Lambda/TorRelay

Backdoor:Lambda/C&CActivity.B

Eine Lambda-Funktion fragt eine IP-Adresse ab, die einem bekannten Command-and-Control-Server zugeordnet wird.

Standard-Schweregrad: Hoch

- Funktion: Lambda Network Activity Monitoring

Diese Erkenntnis informiert Sie darüber, dass eine aufgeführte Lambda-Funktion in Ihrer AWS-Umgebung eine IP-Adresse abfragt, die mit einem bekannten Command and Control (C&C)-Server in Verbindung steht. Die mit der generierten Erkenntnis verknüpfte Lambda-Funktion ist möglicherweise kompromittiert. C&C-Server sind Computer, die Befehle an Mitglieder eines Botnets senden.

Ein Botnet ist eine Sammlung von mit dem Internet verbundenen Geräten, zu denen PCs, Server, mobile Geräte und Geräte des Internets der Dinge gehören können, die mit einem allgemeinen Typ von Malware infiziert sind und von dieser kontrolliert werden. Botnets dienen häufig zum Verteilen von Malware und Sammeln von sich widerrechtlich angeeigneten Informationen, wie z. B. Kreditkartennummern. Je nach Zweck und Struktur des Botnets kann der C&C-Server auch den Befehl erteilen, einen DDoS (Distributed Denial of Service)-Angriff zu starten.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Lambda-Funktion.

CryptoCurrency:Lambda/BitcoinTool.B

Eine Lambda-Funktion fragt eine IP-Adresse ab, die mit einer Aktivität in Zusammenhang mit einer Kryptowährung in Verbindung steht.

Standard-Schweregrad: Hoch

- Funktion: Lambda Network Activity Monitoring

Diese Erkenntnis informiert Sie, dass die aufgeführte Lambda-Funktion in Ihrer AWS-Umgebung eine IP-Adresse abfragt, die mit einer Aktivität in Zusammenhang mit Bitcoin oder einer anderen Kryptowährung in Verbindung steht. Bedrohungsakteure versuchen möglicherweise, die Kontrolle über Lambda-Funktionen zu übernehmen, um sie böswillig für das unbefugte Mining von Kryptowährungen wiederzuverwenden.

Empfehlungen zur Abhilfe:

Wenn Sie diese Lambda-Funktion verwenden, um Kryptowährungen zu minen oder zu verwalten, oder wenn diese Funktion anderweitig an einer Blockchain-Aktivität beteiligt ist, handelt es sich möglicherweise um eine erwartete Aktivität für Ihre Umgebung. Wenn dies in Ihrer AWS-Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Erkenntnistyp-Attribut mit dem Wert CryptoCurrency:Lambda/BitcoinTool.B verwenden. Das zweite Filterkriterium sollte der Lambda-Funktionsname des Features sein, die an der Blockchain-Aktivität beteiligt ist. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Lambda-Funktion.

Trojan:Lambda/BlackholeTraffic

Die Lambda-Funktion versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, der ein bekanntes schwarzes Loch ist.

Standard-Schweregrad: Mittel

- Funktion: Lambda Network Activity Monitoring

Diese Erkenntnis informiert Sie darüber, dass eine aufgeführte Lambda-Funktion in Ihrer AWS-Umgebung versucht, mit der IP-Adresse eines schwarzen Lochs (oder einem Sinkhole) zu kommunizieren. Schwarze Löcher bezeichnen Orte im Netzwerk, an denen eingehender oder

ausgehender Datenverkehr stillschweigend gelöscht wird, ohne die Quelle zu informieren, dass die Daten den vorgesehenen Empfänger nicht erreicht haben. Die IP-Adresse eines schwarzen Lochs gibt einen Hostcomputer an, der nicht ausgeführt wird, oder eine Adresse, der kein Host zugewiesen wurde. Die aufgeführte Lambda-Funktion ist möglicherweise kompromittiert.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Lambda-Funktion.

Trojan:Lambda/DropPoint

Eine Lambda-Funktion versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, von dem bekannt ist, dass er Anmeldeinformationen und andere mithilfe von Malware gestohlene Daten enthält.

Standard-Schweregrad: Mittel

- Funktion: Lambda Network Activity Monitoring

Diese Erkenntnis informiert Sie darüber, dass eine aufgeführte Lambda-Funktion in Ihrer AWS-Umgebung versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, von dem bekannt ist, dass er Anmeldeinformationen und andere mithilfe von Malware gestohlene Daten enthält.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Lambda-Funktion.

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Eine Lambda-Funktion stellt Verbindungen zu einer IP-Adresse auf einer benutzerdefinierten Bedrohungsliste her.

Standard-Schweregrad: Mittel

- Funktion: Lambda Network Activity Monitoring

Diese Erkenntnis informiert Sie darüber, dass eine Lambda-Funktion in Ihrer AWS-Umgebung mit einer IP-Adresse kommuniziert, die auf einer von Ihnen hochgeladenen Bedrohungsliste steht. In GuardDuty besteht eine Bedrohungsliste aus bekannten schädlichen IP-Adressen. GuardDuty generiert Erkenntnisse basierend auf hochgeladenen Bedrohungslisten. Sie können die Details der Bedrohungsliste in den Erkenntnisdetails in der GuardDuty-Konsole einsehen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Lambda-Funktion.

UnauthorizedAccess:Lambda/TorClient

Eine Lambda-Funktion stellt Verbindungen zu einem Tor-Guard oder einem Authority-Knoten her.

Standard-Schweregrad: Hoch

- Funktion: Lambda Network Activity Monitoring

Diese Erkenntnis informiert Sie darüber, dass eine Lambda-Funktion in Ihrer AWS-Umgebung Verbindungen zu einem Tor-Guard oder einem Authority-Knoten herstellt. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor-Guards und Authority-Knoten fungieren als erste Gateways in ein Tor-Netzwerk. Dieser Datenverkehr kann darauf hinweisen, dass diese Lambda-Funktion möglicherweise kompromittiert wurde. Sie fungiert jetzt als Client in einem Tor-Netzwerk.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Lambda-Funktion.

UnauthorizedAccess:Lambda/TorRelay

Eine Lambda-Funktion stellt Verbindungen zu einem Tor-Netzwerk als Tor-Relay her.

Standard-Schweregrad: Hoch

- Funktion: Lambda Network Activity Monitoring

Diese Erkenntnis informiert Sie darüber, dass eine Lambda-Funktion in Ihrer AWS-Umgebung Verbindungen zu einem Tor-Netzwerk auf eine Weise herstellt, die darauf hindeutet, dass sie als Tor-Relay fungiert. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor erhöht die Anonymität der Kommunikation, indem es den möglicherweise illegalen Datenverkehr des Kunden von einem Tor-Relay zu einem anderen weiterleitet.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell kompromittierten Lambda-Funktion.

Erkenntnistypen für Malware Protection

GuardDuty Malware Protection bietet eine einzige Malware-Schutz-Suche für alle Bedrohungen, die beim Scan einer EC2-Instance oder eines Container-Workloads erkannt wurden. Die Erkenntnis umfasst die Gesamtzahl der während des Scans entdeckten Bedrohungen und liefert, basierend auf dem Schweregrad, Details zu den 32 am häufigsten erkannten Bedrohungen. Im Gegensatz zu anderen GuardDuty Ergebnissen werden die Ergebnisse des Malware-Schutzes nicht aktualisiert, wenn dieselbe EC2-Instance oder dieselbe Container-Workload erneut gescannt wird.

Für jeden Scan, bei dem Malware erkannt wird, wird eine neue Malware-Protection-Erkenntnis generiert. Zu den Ergebnissen des Malware-Schutzes gehören Informationen über den entsprechenden Scan, der zu dem Ergebnis geführt hat, sowie GuardDuty zu dem Ergebnis, das diesen Scan ausgelöst hat. Dadurch ist es einfacher, das verdächtige Verhalten mit der erkannten Malware zu korrelieren.

> **Note**
>
> Wenn bösartige Aktivitäten auf einem Container-Workload GuardDuty erkannt werden, generiert der Malware-Schutz kein Ergebnis auf EC2-Ebene.

Die folgenden Ergebnisse beziehen sich speziell auf den GuardDuty Malware-Schutz.

Themen

- Execution:EC2/MaliciousFile
- Execution:ECS/MaliciousFile
- Execution:Kubernetes/MaliciousFile

- Execution:Container/MaliciousFile
- Execution:EC2/SuspiciousFile
- Execution:ECS/SuspiciousFile
- Execution:Kubernetes/SuspiciousFile
- Execution:Container/SuspiciousFile

Execution:EC2/MaliciousFile

Auf einer EC2-Instance wurde eine schädliche Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Merkmal: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der GuardDuty Malware-Schutz-Scan eine oder mehrere schädliche Dateien auf der aufgelisteten EC2-Instance in Ihrer AWS Umgebung entdeckt hat. Die aufgeführte Instance ist möglicherweise kompromittiert. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Execution:ECS/MaliciousFile

Auf einem ECS-Cluster wurde eine bösartige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der GuardDuty Malware-Schutz-Scan eine oder mehrere schädliche Dateien auf einem Container-Workload entdeckt hat, der zu einem ECS-Cluster gehört. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, ist Ihr Container, der zum ECS-Cluster gehört, möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten ECS-Clusters.

Execution:Kubernetes/MaliciousFile

Auf einem Kubernetes-Cluster wurde eine bösartige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der GuardDuty Malware-Schutz-Scan eine oder mehrere schädliche Dateien auf einem Container-Workload entdeckt hat, der zu einem Kubernetes-Cluster gehört. Wenn es sich um einen von EKS verwalteten Cluster handelt, enthalten die Erkenntnisdetails zusätzliche Informationen über die betroffene EKS-Ressource. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, kann Ihr Container-Workload kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Execution:Container/MaliciousFile

In einem eigenständigen Container wurde eine bösartige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der GuardDuty Malware-Schutz-Scan eine oder mehrere schädliche Dateien auf einem Container-Workload entdeckt hat und keine Clusterinformationen identifiziert wurden. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, kann Ihr Container-Workload kompromittiert sein. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten Standalone-Containers.

Execution:EC2/SuspiciousFile

Auf einer EC2-Instance wurde eine verdächtige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der GuardDuty Malware-Schutz-Scan eine oder mehrere verdächtige Dateien auf einer EC2-Instance erkannt hat. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Erkenntnisse vom Typ `SuspiciousFile` deuten darauf hin, dass sich auf einer betroffenen Ressource potenziell unerwünschte Programme wie Adware, Spyware oder Tools mit doppeltem Verwendungszweck befinden. Diese Programme können sich negativ auf Ihre Ressource auswirken oder von Angreifern für böswillige Zwecke verwendet werden. Netzwerktools können beispielsweise von Gegnern legitim oder böswillig als Hacking-Tools verwendet werden, um zu versuchen, Ressourcen zu kompromittieren.

Wenn eine verdächtige Datei erkannt wurde, prüfen Sie, ob Sie davon ausgehen, dass die erkannte Datei in Ihrer AWS Umgebung angezeigt wird. Falls die Datei unerwartet ist, befolgen Sie die Empfehlungen zur Problembehebung im nächsten Abschnitt.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Execution:ECS/SuspiciousFile

Auf einem ECS-Cluster wurde eine verdächtige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der GuardDuty Malware-Schutz-Scan eine oder mehrere verdächtige Dateien in einem Container entdeckt hat, der zu einem ECS-Cluster gehört. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Erkenntnisse vom Typ `SuspiciousFile` deuten darauf hin, dass sich auf einer betroffenen Ressource potenziell unerwünschte Programme wie Adware, Spyware oder Tools mit doppeltem Verwendungszweck befinden. Diese Programme können sich negativ auf Ihre Ressource auswirken oder von Angreifern für böswillige Zwecke verwendet werden. Netzwerktools können beispielsweise von Gegnern legitim oder böswillig als Hacking-Tools verwendet werden, um zu versuchen, Ressourcen zu kompromittieren.

Wenn eine verdächtige Datei erkannt wurde, prüfen Sie, ob Sie damit rechnen, die entdeckte Datei in Ihrer AWS Umgebung zu sehen. Falls die Datei unerwartet ist, befolgen Sie die Empfehlungen zur Problembehebung im nächsten Abschnitt.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, ist Ihr Container, der zum ECS-Cluster gehört, möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten ECS-Clusters.

Execution:Kubernetes/SuspiciousFile

In einem Kubernetes-Cluster wurde eine verdächtige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der GuardDuty Malware-Schutz-Scan eine oder mehrere verdächtige Dateien in einem Container erkannt hat, der zu einem Kubernetes-Cluster gehört. Wenn es sich um einen von EKS verwalteten Cluster handelt, enthalten die Erkenntnisdetails zusätzliche Informationen über die betroffene EKS-Ressource. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Erkenntnisse vom Typ `SuspiciousFile` deuten darauf hin, dass sich auf einer betroffenen Ressource potenziell unerwünschte Programme wie Adware, Spyware oder Tools mit doppeltem Verwendungszweck befinden. Diese Programme können sich negativ auf Ihre Ressource auswirken

oder von Angreifern für böswillige Zwecke verwendet werden. Netzwerktools können beispielsweise von Gegnern legitim oder böswillig als Hacking-Tools verwendet werden, um zu versuchen, Ressourcen zu kompromittieren.

Wenn eine verdächtige Datei erkannt wurde, prüfen Sie, ob Sie damit rechnen, die erkannte Datei in Ihrer AWS Umgebung zu sehen. Falls die Datei unerwartet ist, befolgen Sie die Empfehlungen zur Problembehebung im nächsten Abschnitt.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, kann Ihr Container-Workload kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Execution:Container/SuspiciousFile

In einem eigenständigen Container wurde eine verdächtige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der GuardDuty Malware-Schutz-Scan eine oder mehrere verdächtige Dateien in einem Container ohne Clusterinformationen erkannt hat. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Erkenntnisse vom Typ `SuspiciousFile` deuten darauf hin, dass sich auf einer betroffenen Ressource potenziell unerwünschte Programme wie Adware, Spyware oder Tools mit doppeltem Verwendungszweck befinden. Diese Programme können sich negativ auf Ihre Ressource auswirken oder von Angreifern für böswillige Zwecke verwendet werden. Netzwerktools können beispielsweise von Gegnern legitim oder böswillig als Hacking-Tools verwendet werden, um zu versuchen, Ressourcen zu kompromittieren.

Wenn eine verdächtige Datei erkannt wurde, prüfen Sie, ob Sie damit rechnen, die entdeckte Datei in Ihrer AWS Umgebung zu sehen. Falls die Datei unerwartet ist, befolgen Sie die Empfehlungen zur Problembehebung im nächsten Abschnitt.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, kann Ihr Container-Workload kompromittiert sein. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten Standalone-Containers.

Erkenntnistypen für GuardDuty RDS Protection

GuardDuty RDS Protection erkennt ungewöhnliches Anmeldeverhalten auf Ihrer Datenbank-Instance. Die folgenden Erkenntnisse beziehen sich auf Unterstützte Amazon-Aurora-Datenbanken und weisen immer den Ressourcentyp `RDSDBInstance` auf. Der Schweregrad und die Details der Ergebnisse unterscheiden sich je nach Erkennungstyp.

Themen

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

Ein Benutzer hat sich erfolgreich auf ungewöhnliche Weise bei einer RDS-Datenbank in Ihrem Konto angemeldet.

Standardschweregrad: Variabel

> **Note**
>
> Je nach dem anomalen Verhalten, das mit diesem Ergebnis einhergeht, kann der Standardschweregrad Niedrig, Mittel und Hoch gewählt werden.
>
> - Niedrig – Wenn der mit diesem Ergebnis verknüpfte Benutzername von einer IP-Adresse aus angemeldet ist, die einem privaten Netzwerk zugeordnet ist.
> - Mittel – Wenn der mit diesem Ergebnis verknüpfte Benutzername von einer öffentlichen IP-Adresse aus angemeldet ist.

- Hoch – Wenn es ein einheitliches Muster von fehlgeschlagenen Anmeldeversuchen von öffentlichen IP-Adressen aus gibt, was auf zu freizügige Zugriffsrichtlinien hindeutet.

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Diese Erkenntnis informiert Sie darüber, dass eine ungewöhnliche erfolgreiche Anmeldung in einer RDS-Datenbank in Ihrer AWS-Umgebung beobachtet wurde. Dies kann darauf hindeuten, dass sich ein zuvor unbekannter Benutzer zum ersten Mal bei einer RDS-Datenbank angemeldet hat. Ein häufiges Szenario ist ein interner Benutzer, der sich bei einer Datenbank anmeldet, auf die programmgesteuert von Anwendungen und nicht von einzelnen Benutzern zugegriffen wird.

Diese erfolgreiche Anmeldung wurde vom GuardDuty Machine Learning (ML)-Anomalieentdeckungs-Modell als ungewöhnlich eingestuft. Das ML-Modell bewertet alle Datenbank-Anmeldeereignisse in Ihrer Unterstützte Amazon-Aurora-Datenbanken und identifiziert anomale Ereignisse, die mit den von Gegnern verwendeten Techniken in Verbindung stehen. Das ML-Modell verfolgt verschiedene Faktoren der RDS-Anmeldeaktivität, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifischen Datenbank-Verbindungsdetails, die verwendet wurden. Informationen zu potenziell ungewöhnlichen Anmeldeereignissen finden Sie unter Anomalien aufgrund von RDS-Anmeldeaktivitäten.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, wird empfohlen, das Passwort des zugehörigen Datenbankbenutzers zu ändern und die verfügbaren Audit-Logs auf Aktivitäten zu überprüfen, die von dem anomalen Benutzer ausgeführt wurden. Erkenntnisse mit mittlerem und hohem Schweregrad können darauf hindeuten, dass die Zugriffsrichtlinien für die Datenbank zu freizügig sind und die Anmeldeinformationen der Benutzer möglicherweise offengelegt oder kompromittiert wurden. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen.

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Ein oder mehrere ungewöhnliche fehlgeschlagene Anmeldeversuche wurden in einer RDS-Datenbank in Ihrem Konto beobachtet.

Standard-Schweregrad: Niedrig

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Diese Erkenntnis informiert Sie darüber, dass eine oder mehrere ungewöhnliche erfolgreiche Anmeldungen in einer RDS-Datenbank in Ihrer AWS-Umgebung beobachtet wurde. Fehlgeschlagene Anmeldeversuche von öffentlichen IP-Adressen aus können darauf hindeuten, dass die RDS-Datenbank in Ihrem Konto einem Brute-Force-Angriff durch einen potenziell böswilligen Akteur ausgesetzt war.

Diese erfolgreiche Anmeldung wurde vom GuardDuty Machine Learning (ML)-Anomalieentdeckungs-Modell als ungewöhnlich eingestuft. Das ML-Modell bewertet alle Datenbank-Anmeldeereignisse in Ihrer Unterstützte Amazon-Aurora-Datenbanken und identifiziert anomale Ereignisse, die mit den von Gegnern verwendeten Techniken in Verbindung stehen. Das ML-Modell verfolgt verschiedene Faktoren der RDS-Anmeldeaktivität, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifischen Datenbank-Verbindungsdetails, die verwendet wurden. Informationen zu potenziell ungewöhnlichen RDS-Anmeldeaktivitäten finden Sie unter Anomalien aufgrund von RDS-Anmeldeaktivitäten.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen.

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

Ein Benutzer hat sich nach einem konsistenten Muster ungewöhnlicher fehlgeschlagener Anmeldeversuche erfolgreich von einer öffentlichen IP-Adresse aus auf ungewöhnliche Weise bei einer RDS-Datenbank in Ihrem Konto angemeldet.

Standard-Schweregrad: Hoch

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass bei einer RDS-Datenbank in Ihrer AWS-Umgebung eine ungewöhnliche Anmeldung beobachtet wurde, die auf einen erfolgreichen Brute-Force-Angriff hindeutet. Vor einer anomalen erfolgreichen Anmeldung wurde ein konsistentes Muster ungewöhnlicher fehlgeschlagener Anmeldeversuche beobachtet. Dies deutet darauf hin, dass der Benutzer und das Passwort, die mit der RDS-Datenbank in Ihrem Konto verknüpft sind, möglicherweise kompromittiert wurden und dass möglicherweise ein potenziell böswilliger Akteur auf die RDS-Datenbank zugegriffen hat.

Diese erfolgreiche Anmeldung wurde vom GuardDuty Machine Learning (ML)-Anomalieentdeckungs-Modell als ungewöhnlich eingestuft. Das ML-Modell bewertet alle Datenbank-Anmeldeereignisse in Ihrer Unterstützte Amazon-Aurora-Datenbanken und identifiziert anomale Ereignisse, die mit den von Gegnern verwendeten Techniken in Verbindung stehen. Das ML-Modell verfolgt verschiedene Faktoren der RDS-Anmeldeaktivität, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifischen Datenbank-Verbindungsdetails, die verwendet wurden. Informationen zu potenziell ungewöhnlichen RDS-Anmeldeaktivitäten finden Sie unter Anomalien aufgrund von RDS-Anmeldeaktivitäten.

Empfehlungen zur Abhilfe:

Diese Aktivität weist darauf hin, dass Datenbankanmeldeinformationen möglicherweise offengelegt oder kompromittiert wurden. Es wird empfohlen, das Passwort des zugehörigen Datenbankbenutzers zu ändern und die verfügbaren Prüfungsprotokolle auf Aktivitäten des potenziell kompromittierten Benutzers zu überprüfen. Ein konsistentes Muster ungewöhnlicher fehlgeschlagener Anmeldeversuche deutet auf eine zu freizügige Zugriffsrichtlinie auf die Datenbank hin, oder die Datenbank wurde möglicherweise auch öffentlich zugänglich gemacht. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen.

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

Ein Benutzer hat sich erfolgreich von einer bekannten bösartigen IP-Adresse aus bei einer RDS-Datenbank in Ihrem Konto angemeldet.

Standard-Schweregrad: Hoch

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass eine erfolgreiche RDS-Anmeldeaktivität von einer IP-Adresse aus erfolgte, die mit einer bekannten bösartigen Aktivität in Ihrer AWS-Umgebung in Verbindung steht. Dies deutet darauf hin, dass der Benutzer und das Passwort, die mit der RDS-Datenbank in Ihrem Konto verknüpft sind, möglicherweise kompromittiert wurden und dass möglicherweise ein potenziell böswilliger Akteur auf die RDS-Datenbank zugegriffen hat.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Benutzeranmeldeinformationen möglicherweise offengelegt oder kompromittiert wurden. Es wird empfohlen, das Passwort des zugehörigen Datenbankbenutzers zu ändern und die verfügbaren Prüfungsprotokolle auf Aktivitäten des potenziell kompromittiert Benutzers zu überprüfen. Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen.

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

Eine IP-Adresse, die mit einer bekannten böswilligen Aktivität verknüpft ist, hat erfolglos versucht, sich bei einer RDS-Datenbank in Ihrem Konto anzumelden.

Standard-Schweregrad: Mittel

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass eine IP-Adresse, die mit bekannten böswilligen Aktivitäten in Verbindung steht, versucht hat, sich bei einer RDS-Datenbank in Ihrer AWS-Umgebung anzumelden, dabei aber nicht den richtigen Benutzernamen oder das richtige Passwort angegeben hat. Dies deutet darauf hin, dass ein potenziell böswilliger Akteur versucht, die RDS-Datenbank in Ihrem Konto zu kompromittieren.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen.

Discovery:RDS/MaliciousIPCaller

Eine IP-Adresse, die mit einer bekannten böswilligen Aktivität in Verbindung steht, hat eine RDS-Datenbank in Ihrem Konto untersucht. Es wurde kein Authentifizierungsversuch unternommen.

Standard-Schweregrad: Mittel

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Diese Erkenntnis informiert Sie darüber, dass eine IP-Adresse, die mit einer bekannten bösartigen Aktivität in Verbindung steht, eine RDS-Datenbank in Ihrer AWS Umgebung untersucht hat, obwohl kein Anmeldeversuch unternommen wurde. Dies kann darauf hindeuten, dass ein potenziell böswilliger Akteur versucht, nach einer öffentlich zugänglichen Infrastruktur zu scannen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen.

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

Ein Benutzer hat sich erfolgreich über eine IP-Adresse des Tor-Ausgangsknotens bei einer RDS-Datenbank in Ihrem Konto angemeldet.

Standard-Schweregrad: Hoch

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass sich ein Benutzer erfolgreich von einer IP-Adresse des Tor-Ausgangsknotens aus bei einer RDS-Datenbank in Ihrer AWS-Umgebung angemeldet hat. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf die RDS-Ressourcen hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Benutzeranmeldeinformationen möglicherweise offengelegt oder kompromittiert wurden. Es wird empfohlen, das Passwort des zugehörigen Datenbankbenutzers zu ändern und die verfügbaren Prüfungsprotokolle auf Aktivitäten des potenziell kompromittiert Benutzers zu überprüfen. Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen.

CredentialAccess:RDS/TorIPCaller.FailedLogin

Eine Tor-IP-Adresse hat erfolglos versucht, sich bei einer RDS-Datenbank in Ihrem Konto anzumelden.

Standard-Schweregrad: Mittel

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass die IP-Adresse eines Tor-Ausgangsknotens versucht hat, sich bei einer RDS-Datenbank in Ihrer AWS-Umgebung anzumelden, aber nicht den richtigen Benutzernamen oder das richtige Passwort angegeben hat. Tor ist eine Software, die anonyme

Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf die RDS-Ressourcen hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen.

Discovery:RDS/TorIPCaller

Eine IP-Adresse des Tor-Ausgangsknotens hat eine RDS-Datenbank in Ihrem Konto untersucht, es wurde kein Authentifizierungsversuch unternommen.

Standard-Schweregrad: Mittel

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Diese Erkenntnis informiert Sie darüber, dass die IP-Adresse eines Tor-Ausgangsknotens eine RDS-Datenbank in Ihrer AWS-Umgebung untersucht hat, obwohl kein Anmeldeversuch unternommen wurde. Dies kann darauf hindeuten, dass ein potenziell böswilliger Akteur versucht, nach einer öffentlich zugänglichen Infrastruktur zu scannen. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf die RDS-Ressourcen in Ihrem Konto hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen

zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen.

Runtime Monitoring: Typen finden

Amazon GuardDuty generiert die folgenden Runtime Monitoring-Ergebnisse, um auf potenzielle Bedrohungen hinzuweisen, die auf dem Verhalten von Amazon EC2 EC2-Hosts und Containern in Ihren Amazon EKS-Clustern, Fargate- und Amazon ECS-Workloads und Amazon EC2 EC2-Instances auf Betriebssystemebene basieren.

> **Note**
>
> Die Erkenntnistypen der Laufzeit-Überwachung basieren auf den Laufzeit-Protokollen, die von Hosts gesammelt wurden. Die Protokolle enthalten Felder wie Dateipfade, die möglicherweise von einem böswilligen Akteur kontrolliert werden. Diese Felder sind auch in GuardDuty den Ergebnissen enthalten, um den Laufzeitkontext bereitzustellen. Wenn Sie die Ergebnisse von Runtime Monitoring außerhalb der GuardDuty Konsole verarbeiten, müssen Sie die Suchfelder bereinigen. Sie können z. B. Erkenntnisfelder HTML-kodieren, wenn Sie sie auf einer Webseite anzeigen.

Themen

- CryptoCurrency:Runtime/BitcoinTool.B
- Backdoor:Runtime/C&CActivity.B
- UnauthorizedAccess:Runtime/TorRelay
- UnauthorizedAccess:Runtime/TorClient
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/DropPoint
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Backdoor:Runtime/C&CActivity.B!DNS
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS

- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- UnauthorizedAccess:Runtime/MetadataDNSRebind
- Execution:Runtime/NewBinaryExecuted
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- DefenseEvasion:Runtime/ProcessInjection.Proc
- DefenseEvasion:Runtime/ProcessInjection.Ptrace
- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite
- Execution:Runtime/ReverseShell
- DefenseEvasion:Runtime/FilelessExecution
- Impact:Runtime/CryptoMinerExecuted
- Execution:Runtime/NewLibraryLoaded
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Execution:Runtime/SuspiciousTool
- Execution:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/PtraceAntiDebugging
- Execution:Runtime/MaliciousFileExecuted

CryptoCurrency:Runtime/BitcoinTool.B

Eine Amazon-EC2-Instance oder ein Container fragt eine IP-Adresse ab, die mit einer Aktivität in Zusammenhang mit einer Kryptowährung in Verbindung steht.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance oder ein Container in Ihrer AWS -Umgebung eine IP-Adresse abfragt, die mit einer Kryptowährungsaktivität in Verbindung steht. Bedrohungsakteure können versuchen, die Kontrolle über Datenverarbeitungsressourcen zu übernehmen, um sie böswillig für das unerlaubte Mining von Kryptowährungen umzuwidmen.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2-Instance oder einen Container verwenden, um Kryptowährung zu minen oder zu verwalten, oder einer von beiden anderweitig in Blockchain-Aktivitäten involviert ist, könnte die CryptoCurrency:Runtime/BitcoinTool.B-Erkenntnis eine erwartete Aktivität für Ihre Umgebung darstellen. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für dieses Ergebnis einzurichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Filterkriterium sollte das Attribut Erkenntnistyp mit dem Wert `CryptoCurrency:Runtime/BitcoinTool.B` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance oder die Container-Image-ID des Containers sein, der an Aktivitäten im Zusammenhang mit Kryptowährungen oder Blockchain beteiligt ist. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Backdoor:Runtime/C&CActivity.B

Eine Amazon-EC2-Instance oder ein Container fragt eine IP-Adresse ab, die mit einem bekannten Command-and-Control-Server verbunden ist.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance oder ein Container in Ihrer AWS -Umgebung eine IP-Adresse abfragt, die mit einem bekannten Command-and-Control (C&C)-Server in Verbindung steht. Die aufgeführte Instance oder der aufgeführte Container sind

möglicherweise gefährdet. Command-and-control-Server sind Computer, die Befehle an Mitglieder eines Botnets senden.

Ein Botnet ist eine Sammlung von mit dem Internet verbundenen Geräten, zu denen PCs, Server, mobile Geräte und Geräte des Internets der Dinge gehören können, die mit einem allgemeinen Typ von Malware infiziert sind und von dieser kontrolliert werden. Botnets dienen häufig zum Verteilen von Malware und Sammeln von sich widerrechtlich angeeigneten Informationen, wie z. B. Kreditkartennummern. Je nach Zweck und Struktur des Botnets kann der C&C-Server auch den Befehl erteilen, einen DDoS (Distributed Denial of Service)-Angriff zu starten.

> **Note**
>
> Wenn die abgefragte IP log4j-bezogen ist, enthalten die Felder der zugehörigen Erkenntnis die folgenden Werte:
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

UnauthorizedAccess:Runtime/TorRelay

Ihre Amazon-EC2-Instance oder Ihr Container stellt Verbindungen mit einem Tor-Netzwerk als Tor-Relays her.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass eine EC2-Instance oder ein Container in Ihrer AWS Umgebung Verbindungen zu einem Tor-Netzwerk auf eine Weise herstellt, die darauf hindeutet, dass

es als Tor-Relay fungiert. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor-Relays erhöhen die Anonymität der Kommunikation, indem sie den möglicherweise illegalen Datenverkehr des Kunden von einem Tor-Relay zu einem anderen weiterleiten.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sieh dir den Ressourcentyp im Ergebnisfenster der GuardDuty Konsole an.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

UnauthorizedAccess:Runtime/TorClient

Ihre Amazon-EC2-Instance oder ein Container stellt Verbindungen mit einem Tor Guard oder einem Authority-Knoten her.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert dich darüber, dass eine EC2-Instance oder ein Container in deiner AWS Umgebung Verbindungen zu einem Tor Guard- oder einem Authority-Knoten herstellt. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor Guards und Authority-Knoten fungieren als erste Gateways in ein Tor-Netzwerk. Dieser Datenverkehr kann darauf hinweisen, dass diese EC2-Instance oder der Container als Client in einem Tor-Netzwerk fungieren. Dieses Ergebnis kann auf einen unbefugten Zugriff auf Ihre AWS Ressourcen hinweisen, mit der Absicht, die wahre Identität des Angreifers zu verbergen.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Trojan:Runtime/BlackholeTraffic

Eine Amazon-EC2-Instance oder ein Container versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, der ein bekanntes schwarzes Loch ist.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieser Befund informiert Sie darüber, dass die aufgelistete EC2-Instance oder ein Container in Ihrer AWS Umgebung möglicherweise kompromittiert ist, weil er versucht, mit der IP-Adresse eines schwarzen Lochs (oder Sink Hole) zu kommunizieren. Schwarze Löcher bezeichnen Orte im Netzwerk, an denen eingehender oder ausgehender Datenverkehr stillschweigend gelöscht wird, ohne die Quelle zu informieren, dass die Daten den vorgesehenen Empfänger nicht erreicht haben. Die IP-Adresse eines schwarzen Lochs gibt einen Hostcomputer an, der nicht ausgeführt wird, oder eine Adresse, der kein Host zugewiesen wurde.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Trojan:Runtime/DropPoint

Eine Amazon-EC2-Instance oder ein Container versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, von dem bekannt ist, dass er Anmeldeinformationen und andere mithilfe von Malware gestohlene Daten enthält.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass eine EC2-Instance oder ein Container in Ihrer AWS Umgebung versucht, mit der IP-Adresse eines Remote-Hosts zu kommunizieren, auf dem sich bekanntermaßen Anmeldeinformationen und andere gestohlene Daten befinden, die von Malware erfasst wurden.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

CryptoCurrency:Runtime/BitcoinTool.B!DNS

Eine Amazon EC2-Instance oder ein Container fragt einen Domainnamen ab, der mit einer Aktivität in Zusammenhang mit einer Kryptowährung in Verbindung steht.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie, dass die aufgeführte EC2-Instance oder ein Container in Ihrer AWS -Umgebung einen Domainnamen abfragt, der mit einer Aktivität in Zusammenhang mit Bitcoin oder einer anderen Kryptowährung in Verbindung steht. Bedrohungsakteure können versuchen, die

Kontrolle über Datenverarbeitungsressourcen zu übernehmen, um sie böswillig für das unerlaubte Mining von Kryptowährungen umzuwidmen.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2-Instance oder den Container verwenden, um Kryptowährung zu minen oder zu verwalten, oder diese Instance anderweitig an der Blockchain-Aktivität beteiligt ist, könnte diese CryptoCurrency:Runtime/BitcoinTool.B!DNS-Erkenntnis erwartete Aktivitäten für Ihre Umgebung repräsentieren. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für dieses Ergebnis einzurichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `CryptoCurrency:Runtime/BitcoinTool.B!DNS` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance oder die Container-Image-ID des Containers sein, der an Aktivitäten im Zusammenhang mit Kryptowährungen oder Blockchain beteiligt ist. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Backdoor:Runtime/C&CActivity.B!DNS

Eine Amazon EC2-Instance oder ein Container fragt einen Domainamen ab, der einem bekannten Command-and-Control-Server zugeordnet wird.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance oder der Container in Ihrer AWS -Umgebung einen Domainnamen abfragt, der mit einem bekannten Command-and-Control (C&C)-Server in Verbindung steht. Die aufgelistete EC2 Instance oder der aufgelistete Container sind möglicherweise kompromittiert. Command-and-control-Server sind Computer, die Befehle an Mitglieder eines Botnets senden.

Ein Botnet ist eine Sammlung von mit dem Internet verbundenen Geräten, zu denen PCs, Server, mobile Geräte und Geräte des Internets der Dinge gehören können, die mit einem allgemeinen Typ von Malware infiziert sind und von dieser kontrolliert werden. Botnets dienen häufig zum Verteilen von Malware und Sammeln von sich widerrechtlich angeeigneten Informationen, wie z. B. Kreditkartennummern. Je nach Zweck und Struktur des Botnets kann der C&C-Server auch den Befehl erteilen, einen DDoS (Distributed Denial of Service)-Angriff zu starten.

> **Note**
>
> Wenn der abgefragte Domainname mit log4j zu tun hat, enthalten die Felder der zugehörigen Erkenntnis die folgenden Werte:
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

> **Note**
>
> Um zu testen, wie dieser Befundtyp GuardDuty generiert wird, können Sie von Ihrer Instance aus eine DNS-Anfrage (`dig`für Linux oder `nslookup` für Windows) für eine Testdomäne stellen`guarddutyc2activityb.com`.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Trojan:Runtime/BlackholeTraffic!DNS

Eine Amazon EC2-Instance oder ein Container fragt einen Domainnamen ab, der an eine die IP-Adresse eines schwarzen Lochs weitergeleitet wird.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance oder ein Container in Ihrer AWS -Umgebung möglicherweise kompromittiert wurde, da sie einen Domainnamen abfragt, der an eine IP-Adresse eines schwarzen Lochs weitergeleitet wird. Schwarze Löcher bezeichnen Orte im Netzwerk, an denen eingehender oder ausgehender Datenverkehr stillschweigend gelöscht wird, ohne die Quelle zu informieren, dass die Daten den vorgesehenen Empfänger nicht erreicht haben.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Trojan:Runtime/DropPoint!DNS

Eine Amazon-EC2-Instance oder ein Container fragt einen Domainnamen eines Remote-Hosts ab, von dem bekannt ist, dass er Anmeldeinformationen und andere mithilfe von Malware gestohlene Daten enthält.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass eine EC2-Instance oder ein Container in Ihrer AWS Umgebung den Domainnamen eines Remote-Hosts abfragt, auf dem sich bekanntermaßen Anmeldeinformationen und andere gestohlene Daten befinden, die von Malware erfasst wurden.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Trojan:Runtime/DGADomainRequest.C!DNS

Eine Amazon-EC2-Instance oder ein Container fragt algorithmisch generierte Domains ab. Solche Domains werden häufig von Malware genutzt und können auf eine kompromittierte EC2-Instance oder Container hinweisen.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance oder der Container in Ihrer AWS -Umgebung versucht, Domain Generation Algorithm (DGA)-Domains abzufragen. Ihre Ressource wurde möglicherweise kompromittiert.

DGAs werden verwendet, um in regelmäßigen Abständen eine große Anzahl an Domainnamen zu generieren, die als Rendezvous Points mit ihren Command-and-Control (C&C)-Servern verwendet werden können. Command-and-Control-Server sind Computer, die Befehle an die Mitglieder eines Botnets senden. Hierbei handelt es sich um eine Ansammlung von mit dem Internet verbundenen Geräten, die infiziert sind und von einer gängigen Malware kontrolliert werden. Die große Anzahl potenzieller Rendezvous Points erschwert ein effektives Stilllegen von Botnets, da infizierte Computer versuchen, einige dieser Domainnamen täglich zu kontaktieren, um Updates oder Befehle zu erhalten.

> **Note**
>
> Dieses Ergebnis basiert auf bekannten DGA-Domänen aus GuardDuty Threat-Intelligence-Feeds.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Trojan:Runtime/DriveBySourceTraffic!DNS

Eine Amazon-EC2-Instance oder ein Container fragt einen Domainnamen eines Remote-Host ab, der eine bekannte Quelle von Drive-By-Download-Angriffen ist.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance oder der Container in Ihrer AWS -Umgebung möglicherweise kompromittiert wurden, da Sie einen Domainnamen von einem Remote-Host abfragt, der eine bekannte Quelle von Drive-By-Download-Angriffen ist. Hierbei handelt es sich um unbeabsichtigte Downloads von Computersoftware aus dem Internet, die eine automatische Installation von Viren, Spyware oder Malware auslösen kann.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Trojan:Runtime/PhishingDomainRequest!DNS

Eine Amazon-EC2-Instance oder ein Container fragt Domains ab, die an Phishing-Angriffen beteiligt sind.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance oder ein Container in Ihrer AWS -Umgebung versucht, eine Domain abzufragen, die an Phishing-Angriffen beteiligt ist. Phishing-Domains werden von jemandem eingerichtet, der sich als rechtmäßige Institution ausgibt, um Personen dazu zu bringen, sensible Daten bereitzustellen, wie beispielsweise personenbezogene Informationen, Bank- und Kreditkartendaten oder Passwörter. Ihre EC2-Instance oder der Container

versucht möglicherweise, sensible Daten abzurufen, die auf einer Phishing-Website gespeichert sind, oder versucht möglicherweise, eine Phishing-Website einzurichten. Die EC2-Instance oder der Container sind möglicherweise kompromittiert.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Impact:Runtime/AbusedDomainRequest.Reputation

Eine Amazon-EC2-Instance oder ein Container fragt einen Domainnamen mit niedriger Reputation ab, der mit bekanntermaßen missbrauchten Domains verknüpft ist.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance oder der Container in Ihrer AWS -Umgebung einen Domainnamen mit niedriger Reputation abfragt, der mit bekanntermaßen missbrauchten Domains oder IP-Adressen verknüpft ist. Beispiele für missbrauchte Domains sind Top-Level-Domainnamen (TLDs) und Second-Level-Domainnamen (2LDs), die kostenlose Subdomain-Registrierungen bieten, sowie dynamische DNS-Anbieter. Bedrohungsakteure nutzen diese Services in der Regel, um Domains kostenlos oder zu geringen Kosten zu registrieren. Bei Domains mit geringer Reputation in dieser Kategorie kann es sich auch um abgelaufene Domains handeln, die auf die Parking-IP-Adresse eines Registrars zurückgehen und daher möglicherweise nicht mehr aktiv sind. Bei einer Parking-IP leitet ein Registrar den Verkehr für Domains weiter, die mit keinem Service verknüpft wurden. Die aufgelistete Amazon-EC2-Instance oder der Container können kompromittiert sein, da Bedrohungsakteure diese Registrare oder Services häufig für C&C und die Verbreitung von Malware nutzen.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Impact:Runtime/BitcoinDomainRequest.Reputation

Eine Amazon-EC2-Instance oder ein Container fragt einen Domainnamen ab, der mit einer Aktivität in Zusammenhang mit einer Kryptowährung in Verbindung steht.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance oder der Container in Ihrer AWS -Umgebung einen Domainnamen abfragt, der mit einer Aktivität in Zusammenhang mit Bitcoin oder einer anderen Kryptowährung in Verbindung steht. Bedrohungsakteure können versuchen, die Kontrolle über Datenverarbeitungsressourcen zu übernehmen, um sie böswillig für das unerlaubte Mining von Kryptowährungen umzuwidmen.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2-Instance oder den Container verwenden, um Kryptowährung zu minen oder zu verwalten, oder diese Instance anderweitig an Blockchain-Aktivitäten beteiligt ist, könnte diese Erkenntnis erwartete Aktivitäten für Ihre Umgebung repräsentieren. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für dieses Ergebnis einzurichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen.

Das erste Filterkriterium sollte das Attribut Erkenntnistyp mit dem Wert `Impact:Runtime/BitcoinDomainRequest.Reputation` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance oder die Container-Image-ID des Containers sein, der an Aktivitäten im Zusammenhang mit Kryptowährung oder Blockchain beteiligt ist. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Impact:Runtime/MaliciousDomainRequest.Reputation

Eine Amazon-EC2-Instance oder ein Container fragt eine Domain mit niedriger Reputation ab, die mit bekannten bösartigen Domains verknüpft ist.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance oder der Container in Ihrer AWS -Umgebung einen Domainnamen mit niedriger Reputation abfragt, der mit bekannten bösartigen Domains oder IP-Adressen verknüpft ist. Beispielsweise können Domains mit einer bekannten Sinkhole-IP-Adresse verknüpft sein. Sinkhole-Domains sind Domains, die zuvor von einem Bedrohungsakteur kontrolliert wurden, und Anfragen an sie können darauf hinweisen, dass die Instance kompromittiert wurde. Diese Domains können auch mit bekannten böswilligen Kampagnen oder Algorithmen zur Domain-Generierung korreliert sein.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Impact:Runtime/SuspiciousDomainRequest.Reputation

Eine Amazon-EC2-Instance oder ein Container fragt einen Domainnamen mit geringer Reputation ab, der aufgrund seines Alters oder seiner geringen Beliebtheit verdächtig ist.

Standard-Schweregrad: Niedrig

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance oder der Container in Ihrer AWS -Umgebung einen Domainnamen mit niedriger Reputation abfragt, bei dem der Verdacht besteht, dass er bösartig ist. Es wurden Merkmale dieser Domain festgestellt, die mit zuvor beobachteten bösartigen Domains übereinstimmten. Unser Reputationsmodell konnte sie jedoch nicht definitiv mit einer bekannten Bedrohung in Verbindung bringen. Diese Domains werden in der Regel neu beobachtet oder erhalten nur wenig Datenverkehr.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

UnauthorizedAccess:Runtime/MetadataDNSRebind

Eine Amazon-EC2-Instance oder ein Container führen DNS-Lookups durch, die in den Instance-Metadatenservice aufgelöst werden.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

> **Note**
>
> Derzeit wird dieser Befundtyp nur für die AMD64-Architektur unterstützt.

Dieses Ergebnis informiert Sie darüber, dass eine EC2-Instance oder ein Container in Ihrer AWS Umgebung eine Domain abfragt, die in die EC2-Metadaten-IP-Adresse (169.254.169.254) aufgelöst wird. Eine solche DNS-Abfrage kann darauf hinweisen, dass die Instance das Ziel einer DNS-Neubindung-Technik ist. Diese Technik kann verwendet werden, um Metadaten von einer EC2-Instance abzurufen, einschließlich der mit der Instance verknüpften IAM-Anmeldeinformationen.

Bei der DNS-Neubindung wird eine Anwendung, die auf der EC2-Instance läuft, dazu gebracht, Rückgabedaten von einer URL zu laden, wobei der Domainname in der URL in die IP-Adresse der EC2-Metadaten (`169.254.169.254`) aufgelöst wird. Dies bewirkt, dass die Anwendung auf EC2-Metadaten zugreift und sie möglicherweise für den Angreifer verfügbar macht.

Der Zugriff auf EC2-Metadaten mit DNS-Neubindung ist nur möglich, wenn auf der EC2-Instance eine anfällige Anwendung ausgeführt wird, die das Einfügen von URLs ermöglicht, oder wenn ein menschlicher Benutzer in einem Webbrowser, der auf der EC2-Instance ausgeführt wird, auf die URL zugreift.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Prüfen Sie als Reaktion auf diese Erkenntnis, ob auf der EC2-Instance oder dem Container eine anfällige Anwendung ausgeführt wird, oder ob ein menschlicher Benutzer über einen Browser auf die in der Erkenntnis angegebene Domain zugegriffen hat. Wenn die Ursache eine anfällige Anwendung ist, beheben Sie die Schwachstelle. Wenn ein Benutzer die identifizierte Domain aufgerufen hat, blockieren Sie die Domain oder verhindern Sie, dass Benutzer darauf zugreifen. Wenn Sie in dieser Erkenntnis einen Zusammenhang mit einem der obigen Fälle feststellen, sollten Sie die mit der EC2-Instance verknüpfte Sitzung widerrufen.

Manche AWS Kunden ordnen die Metadaten-IP-Adresse bewusst einem Domainnamen auf ihren autoritativen DNS-Servern zu. Wenn dies in Ihrer -Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei

Filterkriterien bestehen. Das erste Filterkriterium sollte das Attribut Erkenntnistyp mit dem Wert `UnauthorizedAccess:Runtime/MetaDataDNSRebind` verwenden. Das zweite Filterkriterium sollte die DNS-Anforderungs-Domain oder die Container-Image-ID des Containers sein. Das zweite Filterkriterium sollte die DNS-Anforderungs-Domain sein, und der Wert sollte mit der Domain übereinstimmen, die Sie der Metadaten-IP-Adresse zugeordnet haben (`169.254.169.254`). Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Execution:Runtime/NewBinaryExecuted

Eine neu erstellte oder kürzlich geänderte Binärdatei in einem Container wurde ausgeführt.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass eine neu erstellte oder kürzlich geänderte Binärdatei in einem Container ausgeführt wurde. Es ist eine bewährte Methode, Container zur Laufzeit unveränderlich zu halten. Binärdateien, Skripten oder Bibliotheken sollten während der Lebensdauer des Containers nicht erstellt oder geändert werden. Dieses Verhalten deutet darauf hin, dass ein böswilliger Akteur, der Zugriff auf den Container erlangt hat, im Rahmen der potenziellen Sicherheitslücke Malware oder andere Software heruntergeladen und ausgeführt hat. Diese Art von Aktivität könnte zwar ein Hinweis auf eine Gefährdung sein, ist aber auch ein übliches Nutzungsmuster. GuardDuty Verwendet daher Mechanismen zur Identifizierung verdächtiger Instanzen dieser Aktivität und generiert diesen Befundtyp nur für verdächtige Fälle.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

PrivilegeEscalation:Runtime/DockerSocketAccessed

Ein Prozess in einem Container kommuniziert über den Docker-Socket mit dem Docker-Daemon.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Der Docker-Socket ist ein Unix-Domain-Socket, den Docker-Daemon (`dockerd`) verwendet, um mit seinen Clients zu kommunizieren. Ein Client kann verschiedene Aktionen ausführen, z. B. das Erstellen von Containern, indem er über den Docker-Socket mit dem Docker-Daemon kommuniziert. Es ist verdächtig, dass ein Container-Prozess auf den Docker-Socket zugreift. Ein Container-Prozess kann den Container verlassen und Zugriff auf Host-Ebene erhalten, indem er mit dem Docket-Socket kommuniziert und einen privilegierten Container erstellt.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

PrivilegeEscalation:Runtime/RuncContainerEscape

Ein Versuch, einem Container über RunC zu entkommen, wurde festgestellt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

RunC ist die Low-Level-Container-Runtime, die Container-Laufzeiten auf hoher Ebene wie Docker und Containerd verwenden, um Container zu erzeugen und auszuführen. RunC wird immer mit Root-Rechten ausgeführt, da es die Low-Level-Aufgabe, einen Container zu erstellen, ausführen muss. Ein

Bedrohungsakteur kann sich Zugriff auf Host-Ebene verschaffen, indem er eine Sicherheitslücke in der RunC-Binärdatei entweder modifiziert oder ausnutzt.

Dieses Ergebnis deckt Änderungen an der RunC-Binärdatei und mögliche Versuche auf, die folgenden RunC-Schwachstellen auszunutzen:

- CVE-2019-5736— CVE-2019-5736 Bei der Ausnutzung von wird die RunC-Binärdatei aus einem Container heraus überschrieben. Dieses Ergebnis wird ausgelöst, wenn die RunC-Binärdatei durch einen Prozess in einem Container geändert wird.
- CVE-2024-21626— CVE-2024-21626 Bei der Ausnutzung von wird das aktuelle Arbeitsverzeichnis (CWD) oder ein Container auf einen offenen Dateideskriptor gesetzt. `/proc/self/fd/`*`FileDescriptor`* Dieser Befund wird aufgerufen, wenn ein Container-Prozess erkannt wird, unter dem sich ein aktuelles Arbeitsverzeichnis `/proc/self/fd/` befindet, z. B. `/proc/self/fd/7`

Dieses Ergebnis kann darauf hindeuten, dass ein böswilliger Akteur versucht hat, einen der folgenden Containertypen auszunutzen:

- Ein neuer Container mit einem vom Angreifer kontrollierten Image.
- Ein vorhandener Container, auf den der Akteur mit Schreibberechtigungen für die RunC-Binärdatei auf Hostebene zugreifen konnte.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

Es wurde ein Versuch entdeckt, einem Container durch den CGroups Release Agent zu entkommen.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass ein Versuch erkannt wurde, eine Release-Agent-Datei für eine Kontrollgruppe (Cgroup) zu ändern. Linux verwendet Kontrollgruppen (Cgroups), um die Ressourcennutzung einer Reihe von Prozessen einzuschränken, zu berücksichtigen und zu isolieren. Jede Cgroup hat eine Release-Agent-Datei (`release_agent`), ein Skript, das Linux ausführt, wenn ein Prozess innerhalb der Cgroup beendet wird. Die Release-Agent-Datei wird immer auf Host-Ebene ausgeführt. Ein Bedrohungsakteur in einem Container kann zum Host entkommen, indem er beliebige Befehle in die Release-Agent-Datei schreibt, die zu einer Cgroup gehört. Wenn ein Prozess innerhalb dieser Cgroup beendet wird, werden die vom Akteur geschriebenen Befehle ausgeführt.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.Proc

In einem Container oder einer Amazon-EC2-Instance wurde eine Prozessinjektion mithilfe des proc-Dateisystems erkannt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Bei der Prozessinjektion handelt es sich um eine Technik, mit der Bedrohungsakteure Code in Prozesse einschleusen, um Schutzmaßnahmen zu umgehen und möglicherweise Rechte zu erweitern. Das proc-Dateisystem (procfs) ist ein spezielles Dateisystem in Linux, das den virtuellen Speicher eines Prozesses als Datei darstellt. Der Pfad dieser Datei ist `/proc/PID/mem`, wobei `PID` die eindeutige ID des Prozesses ist. Ein Bedrohungsakteur kann in diese Datei schreiben, um Code in den Prozess einzuschleusen. Diese Erkenntnis identifiziert potenzielle Versuche, in diese Datei zu schreiben.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, wurde Ihr Ressourcentyp möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.Ptrace

In einem Container oder einer Amazon-EC2-Instance wurde eine Prozessinjektion mithilfe des ptrace-Systemaufrufs erkannt.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Bei der Prozessinjektion handelt es sich um eine Technik, mit der Bedrohungsakteure Code in Prozesse einschleusen, um Schutzmaßnahmen zu umgehen und möglicherweise Rechte zu erweitern. Ein Prozess kann den ptrace-Systemaufruf verwenden, um Code in einen anderen Prozess einzuschleusen. Diese Erkenntnis identifiziert einen möglichen Versuch, mithilfe des Systemaufrufs ptrace Code in einen Prozess einzuschleusen.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, wurde Ihr Ressourcentyp möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

In einem Container oder einer Amazon-EC2-Instance wurde eine Prozessinjektion durch direktes Schreiben in den virtuellen Speicher erkannt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Bei der Prozessinjektion handelt es sich um eine Technik, mit der Bedrohungsakteure Code in Prozesse einschleusen, um Schutzmaßnahmen zu umgehen und möglicherweise Rechte zu erweitern. Ein Prozess kann einen Systemaufruf wie `process_vm_writev` verwenden, um Code direkt in den virtuellen Speicher eines anderen Prozesses einzuschleusen. Diese Erkenntnis identifiziert einen möglichen Versuch, mithilfe eines Systemaufrufs Code in den virtuellen Speicher eines Prozesses einzuschleusen.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, wurde Ihr Ressourcentyp möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Execution:Runtime/ReverseShell

Ein Prozess in einem Container oder einer Amazon-EC2-Instance hat eine Reverse-Shell erstellt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Eine Reverse-Shell ist eine Shell-Sitzung, die auf einer Verbindung erstellt wird, die vom Zielhost zum Host des Akteurs initiiert wird. Dies ist das Gegenteil einer normalen Shell, die vom Host des Akteurs zum Host des Ziels initiiert wird. Bedrohungsakteure erstellen eine Reverse-Shell, um Befehle auf dem Ziel auszuführen, nachdem sie sich den ersten Zugriff auf das Ziel verschafft haben. Diese Erkenntnis weist auf einen möglichen Versuch hin, eine Reverse-Shell zu erstellen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, wurde Ihr Ressourcentyp möglicherweise kompromittiert.

DefenseEvasion:Runtime/FilelessExecution

Ein Prozess in einem Container oder einer Amazon-EC2-Instance führt Code aus dem Speicher aus.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, wenn ein Prozess mit einer im Speicher befindlichen ausführbaren Datei auf der Festplatte ausgeführt wird. Dabei handelt es sich um eine gängige Technik zur Umgehung von Schutzmaßnahmen, bei der verhindert wird, dass die schädliche ausführbare Datei auf die Festplatte geschrieben wird, um der Erkennung durch Dateisystem-Scans zu entgehen. Diese Technik wird zwar von Schadsoftware verwendet, hat aber auch einige legitime Anwendungsfälle. Eines der Beispiele ist ein just-in-time (JIT-) Compiler, der kompilierten Code in den Speicher schreibt und ihn aus dem Speicher ausführt.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Impact:Runtime/CryptoMinerExecuted

Ein Container oder eine Amazon-EC2-Instance führt eine Binärdatei aus, die mit einer Cryptocurrency-Mining-Aktivität verknüpft ist.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Container oder eine EC2-Instance in Ihrer AWS Umgebung eine Binärdatei ausführt, die mit einer Cryptocurrency-Mining-Aktivität verknüpft ist.

Bedrohungsakteure können versuchen, die Kontrolle über Datenverarbeitungsressourcen zu übernehmen, um sie böswillig für das unerlaubte Mining von Kryptowährungen umzuwidmen.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie in den Ergebnisdetails in der GuardDuty Konsole unter Ressourcentyp und dann unterBehebung der Ergebnisse von Runtime Monitoring.

Execution:Runtime/NewLibraryLoaded

Eine neu erstellte oder kürzlich geänderte Bibliothek wurde von einem Prozess in einen Container geladen.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass eine Bibliothek während der Laufzeit in einem Container erstellt oder geändert und von einem Prozess geladen wurde, der innerhalb des Containers ausgeführt wird. Es ist eine bewährte Methode, Container zur Laufzeit unveränderlich zu halten. Binärdateien, Skripten oder Bibliotheken sollten während der Lebensdauer des Containers nicht erstellt oder geändert werden. Das Laden einer neu erstellten oder geänderten Bibliothek in einen Container kann auf verdächtige Aktivitäten hinweisen. Dieses Verhalten weist auf einen böswilligen Akteur hin, der sich Zugriff auf den Container verschafft und im Rahmen der potenziellen Sicherheitslücke Malware oder andere Software heruntergeladen und ausgeführt hat. Diese Art von Aktivität könnte zwar ein Hinweis auf eine Beeinträchtigung sein, ist aber auch ein übliches Nutzungsmuster. GuardDuty Verwendet daher Mechanismen zur Identifizierung verdächtiger Instanzen dieser Aktivität und generiert diesen Befundtyp nur für verdächtige Fälle.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

Ein Prozess in einem Container hat zur Laufzeit ein Host-Dateisystem gemountet.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Bei mehreren Techniken zur Container-Escape-Methode wird zur Laufzeit ein Host-Dateisystem in einem Container gemountet. Diese Erkenntnis informiert Sie darüber, dass ein Prozess in einem Container möglicherweise versucht hat, ein Host-Dateisystem zu mounten, was auf einen Fluchtversuch zum Host hindeuten kann.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

PrivilegeEscalation:Runtime/UserfaultfdUsage

Ein Prozess verwendete **`userfaultfd`**-Systemaufrufe, um Seitenfehler im Benutzerbereich zu behandeln.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Typischerweise werden Seitenfehler vom Kernel im Kernel-Space behandelt. Ein `userfaultfd`-Systemaufruf ermöglicht es einem Prozess jedoch, Seitenfehler in einem Dateisystem in der Benutzerumgebung zu behandeln. Dies ist eine nützliches Feature, die die Implementierung von Dateisystemen in der Benutzerumgebung ermöglicht. Andererseits kann sie auch von einem

potenziell bösartigen Prozess verwendet werden, um den Kernel von der Benutzerumgebung aus zu unterbrechen. Das Unterbrechen des Kernels mithilfe eines `userfaultfd`-Systemaufrufs ist eine gängige Ausnutzungstechnik, um Race-Fenster zu verlängern, während die Kernel-Race-Bedingungen ausgenutzt werden. Die Verwendung von `userfaultfd` kann auf verdächtige Aktivitäten auf der Amazon Elastic Compute Cloud (Amazon EC2)-Instance hinweisen.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Execution:Runtime/SuspiciousTool

Ein Container oder eine Amazon EC2 EC2-Instance führt eine Binärdatei oder ein Binärskript aus, das häufig in offensiven Sicherheitsszenarien wie Pentesting verwendet wird.

Standardschweregrad: Variabel

Der Schweregrad dieser Feststellung kann entweder hoch oder niedrig sein, je nachdem, ob das erkannte verdächtige Tool als doppelt oder ausschließlich für anstößige Zwecke verwendet wird.

- Feature: Laufzeit-Überwachung

Dieser Befund informiert Sie darüber, dass ein verdächtiges Tool auf einer EC2-Instance oder einem EC2-Container in Ihrer AWS Umgebung ausgeführt wurde. Dazu gehören Tools, die bei Pentesting-Projekten verwendet werden, auch bekannt als Backdoor-Tools, Netzwerkscanner und Netzwerk-Sniffer. All diese Tools können in harmlosen Kontexten eingesetzt werden, werden aber auch häufig von Bedrohungsakteuren mit böswilligen Absichten eingesetzt. Die Beobachtung anstößiger Sicherheitstools könnte darauf hindeuten, dass die zugehörige EC2-Instance oder der zugehörige EC2-Container kompromittiert wurde.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext, sodass dieser Befund nur generiert wird, wenn die zugehörige Aktivität und der zugehörige Kontext potenziell verdächtig sind.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Execution:Runtime/SuspiciousCommand

Ein verdächtiger Befehl wurde auf einer Amazon EC2 EC2-Instance oder einem Container ausgeführt, der auf eine Kompromittierung hindeutet.

Standardschweregrad: Variabel

Je nach Auswirkung des beobachteten Schadmusters kann der Schweregrad dieses Erkennungstyps entweder niedrig, mittel oder hoch sein.

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein verdächtiger Befehl ausgeführt wurde, und weist darauf hin, dass eine Amazon EC2 EC2-Instance oder ein Container in Ihrer AWS Umgebung kompromittiert wurde. Dies kann bedeuten, dass entweder eine Datei von einer verdächtigen Quelle heruntergeladen und dann ausgeführt wurde oder dass ein laufender Prozess in seiner Befehlszeile ein bekanntes bösartiges Muster anzeigt. Dies deutet weiter darauf hin, dass Malware auf dem System ausgeführt wird.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext, sodass dieser Befund nur dann generiert wird, wenn die zugehörige Aktivität und der zugehörige Kontext potenziell verdächtig sind.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

DefenseEvasion:Runtime/SuspiciousCommand

Ein Befehl wurde auf der aufgelisteten Amazon EC2 EC2-Instance oder einem Container ausgeführt. Er versucht, einen Linux-Abwehrmechanismus wie eine Firewall oder wichtige Systemdienste zu ändern oder zu deaktivieren.

Standardschweregrad: Variabel

Je nachdem, welcher Abwehrmechanismus geändert oder deaktiviert wurde, kann der Schweregrad dieses Erkennungstyps entweder hoch, mittel oder niedrig sein.

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Befehl ausgeführt wurde, der versucht, einen Angriff vor den Sicherheitsdiensten des lokalen Systems zu verbergen. Dazu gehören Aktionen wie das Deaktivieren der Unix-Firewall, das Ändern lokaler IP-Tabellen, das Entfernen von crontab Einträgen, das Deaktivieren eines lokalen Dienstes oder die Übernahme der `LDPreload` Funktion. Jede Änderung ist äußerst verdächtig und ein potenzieller Hinweis auf eine Gefährdung. Daher erkennen oder verhindern diese Mechanismen weitere Beeinträchtigungen des Systems.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext, sodass dieser Befund nur dann generiert wird, wenn die zugehörige Aktivität und der zugehörige Kontext potenziell verdächtig sind.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

DefenseEvasion:Runtime/PtraceAntiDebugging

Ein Prozess in einem Container oder einer Amazon EC2 EC2-Instance hat mithilfe des ptrace-Systemaufrufs eine Anti-Debugging-Maßnahme ausgeführt.

Standard-Schweregrad: Niedrig

- Feature: Laufzeit-Überwachung

Dieses Ergebnis zeigt, dass ein Prozess, der auf einer Amazon EC2 EC2-Instance oder einem Container in Ihrer AWS Umgebung läuft, den ptrace-Systemaufruf mit der `PTRACE_TRACEME` Option verwendet hat. Diese Aktivität würde dazu führen, dass sich ein angehängter Debugger vom laufenden Prozess trennt. Wenn kein Debugger angehängt ist, hat dies keine Wirkung. Die Aktivität an sich erweckt jedoch Verdacht. Dies könnte darauf hindeuten, dass Malware auf dem System ausgeführt wird. Malware verwendet häufig Anti-Debugging-Techniken, um Analysen zu umgehen. Diese Techniken können zur Laufzeit erkannt werden.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext, sodass dieses Ergebnis nur dann generiert wird, wenn die zugehörige Aktivität und der zugehörige Kontext potenziell verdächtig sind.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Execution:Runtime/MaliciousFileExecuted

Eine bekannte bösartige ausführbare Datei wurde auf einer Amazon EC2 EC2-Instance oder einem Container ausgeführt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass eine bekannte bösartige ausführbare Datei auf einer Amazon EC2 EC2-Instance oder einem Container in Ihrer AWS Umgebung ausgeführt wurde. Dies ist ein starker Indikator dafür, dass die Instance oder der Container potenziell kompromittiert wurde und dass Malware ausgeführt wurde.

Malware verwendet häufig Anti-Debugging-Techniken, um Analysen zu umgehen, und diese Techniken können zur Laufzeit erkannt werden.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext, sodass dieses Ergebnis nur dann generiert wird, wenn die zugehörige Aktivität und der zugehörige Kontext potenziell verdächtig sind.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

GuardDuty S3-Suchttypen

Die folgenden Ergebnisse sind spezifisch für Amazon S3 S3-Ressourcen und haben den Ressourcentyp, `S3Bucket` ob es sich bei der Datenquelle um CloudTrail Datenereignisse für S3 oder `AccessKey` um CloudTrail Verwaltungsereignisse handelt. Der Schweregrad und die Details der Ergebnisse unterscheiden sich je nach Ergebnistyp und Berechtigung, die dem Bucket zugeordnet sind.

Die hier aufgeführten Erkenntnisse beinhalten die Datenquellen und Modelle, die zur Generierung dieses Erkenntnistyps verwendet wurden. Weitere Informationen zu Datenquellen und Modellen finden Sie unter Grundlegende Datenquellen.

> **Important**
>
> Ergebnisse mit einer Datenquelle für CloudTrail Datenereignisse für S3 werden nur generiert, wenn Sie den S3-Schutz aktiviert haben GuardDuty. Der S3-Schutz ist standardmäßig für alle Konten aktiviert, die nach dem 31. Juli 2020 erstellt wurden. Weitere Informationen zur Aktivierung oder Deaktivierung von S3-Schutz finden Sie unter Amazon S3 S3-Schutz bei Amazon GuardDuty

Für alle `S3Bucket`-Arten von Erkenntnissen wird empfohlen, die Berechtigungen für den betreffenden Bucket und die Berechtigungen aller Benutzer, die an dem Erkenntniss beteiligt waren,

zu überprüfen. Falls die Aktivität unerwartet ist, lesen Sie die Empfehlungen zur Problembehebung unter Behebung eines potenziell gefährdeten S3-Buckets.

Themen

Discovery:S3/AnomalousBehavior

Eine API, die häufig zum Auffinden von S3-Objekten verwendet wird, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Niedrig

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass eine IAM-Entität eine S3-API aufgerufen hat, um S3-Buckets in Ihrer Umgebung zu erkennen, z. B. `ListObjects`. Diese Art von Aktivität steht im Zusammenhang mit der Erkennungsphase eines Angriffs, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihre AWS Umgebung für einen umfassenderen Angriff anfällig ist. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise ruft eine IAM-Entität ohne vorherige Historie eine S3-API auf, oder eine IAM-Entität ruft eine S3-API von einem ungewöhnlichen Ort aus auf.

Diese API wurde durch das ML-Modell (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Techniken von Angreifern in Verbindung gebracht werden. Es verfolgt verschiedene Faktoren der API-Anfragen, wie z. B. den Nutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, die spezifische API, die angefordert wurde, den angeforderten Bucket und die Anzahl der durchgeführten API-Aufrufe. Weitere Informationen darüber, welche Faktoren der API-Anforderung für die Benutzeridentität, die die Anforderung aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Discovery:S3/MaliciousIPCaller

Eine S3-API, die häufig zur Erkennung von Ressourcen in einer AWS Umgebung verwendet wird, wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass ein S3-API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit der Erkennungsphase eines Angriffs in Verbindung gebracht, in der ein Angreifer

Informationen über Ihre AWS Umgebung sammelt. Beispiele hierfür sind `GetObjectAcl` und `ListObjects`.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Discovery:S3/MaliciousIPCaller.Custom

Eine S3-API wurde von einer IP-Adresse aufgerufen, die sich auf einer benutzerdefinierten Bedrohungsliste befindet.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass eine S3-API, wie z. B. `GetObjectAcl` oder `ListObjects` von einer IP-Adresse aufgerufen wurde, die auf einer von Ihnen hochgeladenen Bedrohungsliste steht. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Die beobachtete API wird häufig mit der Erkennungsphase eines Angriffs in Verbindung gebracht, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihre AWS -Umgebung für einen umfassenderen Angriff anfällig ist.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Discovery:S3/TorIPCaller

Eine S3-API wurde von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass eine S3-API, wie `GetObjectAcl` oder`ListObjects`, von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen wurde. Diese Art von Aktivität steht im Zusammenhang mit der Erkennungsphase eines Angriffs, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihre AWS Umgebung für einen umfassenderen Angriff anfällig ist. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf Ihre AWS Ressourcen hinweisen, um die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Exfiltration:S3/AnomalousBehavior

Eine IAM-Entität hat eine S3-API auf verdächtige Weise aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass eine IAM-Entität API-Aufrufe tätigt, die einen S3-Bucket betreffen, und dass sich diese Aktivität von der festgelegten Basisaktivität dieser Entität unterscheidet. Der in dieser Aktivität verwendete API-Aufruf steht im Zusammenhang mit der Exfiltrationsphase eines Angriffs, in der ein Angreifer versucht, Daten zu sammeln. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise ruft eine IAM-Entität ohne vorherige Historie eine S3-API auf, oder eine IAM-Entität ruft eine S3-API von einem ungewöhnlichen Ort aus auf.

Diese API wurde anhand des ML-Modells (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Techniken von Angreifern in Verbindung gebracht werden. Es verfolgt verschiedene Faktoren der API-Anfragen, wie z. B. den Nutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, die spezifische API, die angefordert wurde,

den angeforderten Bucket und die Anzahl der durchgeführten API-Aufrufe. Weitere Informationen darüber, welche Faktoren der API-Anforderung für die Benutzeridentität, die die Anforderung aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Exfiltration:S3/MaliciousIPCaller

Eine S3-API, die üblicherweise zum Sammeln von Daten aus einer AWS Umgebung verwendet wird, wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass ein S3-API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit Exfiltrationstaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten aus Ihrem Netzwerk zu sammeln. Beispiele hierfür sind `GetObject` und `CopyObject`.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Impact:S3/AnomalousBehavior.Delete

Eine IAM-Entität hat eine S3-API aufgerufen, die versucht, Daten auf verdächtige Weise zu löschen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass eine IAM-Entität in Ihrer AWS Umgebung API-Aufrufe tätigt, die einen S3-Bucket betreffen, und dass sich dieses Verhalten von der festgelegten Baseline dieser Entität unterscheidet. Der in dieser Aktivität verwendete API-Aufruf steht im Zusammenhang mit einem Angriff, bei dem versucht wird, Daten zu löschen. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise ruft eine IAM-Entität ohne vorherige Historie eine S3-API auf, oder eine IAM-Entität ruft eine S3-API von einem ungewöhnlichen Ort aus auf.

Diese API wurde durch das ML-Modell (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Techniken von Angreifern in Verbindung gebracht werden. Es verfolgt verschiedene Faktoren der API-Anfragen, wie z. B. den Nutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, die spezifische API, die angefordert wurde, den angeforderten Bucket und die Anzahl der durchgeführten API-Aufrufe. Weitere Informationen darüber, welche Faktoren der API-Anforderung für die Benutzeridentität, die die Anforderung aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Wir empfehlen eine Prüfung des Inhalts Ihres S3-Buckets, um festzustellen, ob die vorherige Objektversion wiederhergestellt werden kann oder sollte.

Impact:S3/AnomalousBehavior.Permission

Eine API, die häufig zum Festlegen der Berechtigungen für Zugriffssteuerungslisten (ACL) verwendet wird, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass eine IAM-Entität in Ihrer AWS Umgebung eine Bucket-Richtlinie oder ACL für die aufgelisteten S3-Buckets geändert hat. Durch diese Änderung können Ihre S3-Buckets allen authentifizierten Benutzern öffentlich zugänglich gemacht werden. AWS

Diese API wurde durch das ML-Modell (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Techniken von Angreifern in Verbindung gebracht werden. Es verfolgt verschiedene Faktoren der API-Anfragen, wie z. B. den Nutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, die spezifische API, die angefordert wurde, den angeforderten Bucket und die Anzahl der durchgeführten API-Aufrufe. Weitere Informationen darüber, welche Faktoren der API-Anforderung für die Benutzeridentität, die die Anforderung aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Wir empfehlen eine Prüfung des Inhalts Ihres S3-Buckets, um sicherzustellen, dass kein unerwarteter öffentlicher Zugriff auf Objekte gewährt wurde.

Impact:S3/AnomalousBehavior.Write

Eine IAM-Entität hat eine S3-API aufgerufen, die versucht, Daten auf verdächtige Weise zu schreiben.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass eine IAM-Entität in Ihrer AWS Umgebung API-Aufrufe tätigt, die einen S3-Bucket betreffen, und dass sich dieses Verhalten von der festgelegten Baseline dieser Entität unterscheidet. Der in dieser Aktivität verwendete API-Aufruf steht im Zusammenhang mit einem Angriff, bei dem versucht wird, Daten zu schreiben. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise ruft eine IAM-Entität ohne vorherige Historie eine S3-API auf, oder eine IAM-Entität ruft eine S3-API von einem ungewöhnlichen Ort aus auf.

Diese API wurde durch das ML-Modell (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Techniken von Angreifern in Verbindung gebracht werden. Es verfolgt verschiedene Faktoren der API-Anfragen, wie z. B. den Nutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, die spezifische API, die angefordert wurde, den angeforderten Bucket und die Anzahl der durchgeführten API-Aufrufe. Weitere Informationen darüber, welche Faktoren der API-Anforderung für die Benutzeridentität, die die Anforderung aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Wir empfehlen eine Prüfung des Inhalts Ihres S3-Buckets, um sicherzustellen, dass bei diesem API-Aufruf keine schädlichen oder unautorisierten Daten geschrieben wurden.

Impact:S3/MaliciousIPCaller

Eine S3-API, die häufig zur Manipulation von Daten oder Prozessen in einer AWS Umgebung verwendet wird, wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass ein S3-API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit Schlagtaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten in Ihrer Umgebung zu manipulieren, zu unterbrechen oder zu zerstören. AWS Beispiele hierfür sind `PutObject` und `PutObjectAcl`.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv

genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

PenTest:S3/KaliLinux

Eine S3-API wurde von einem Kali-Linux-Computer aus aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass ein Computer, auf dem Kali Linux ausgeführt wird, S3-API-Aufrufe mit Anmeldeinformationen durchführt, die zu Ihrem AWS Konto gehören. Ihre Anmeldeinformationen wurden möglicherweise kompromittiert. Kali Linux ist ein beliebtes Tool für Penetrationstests, das von Sicherheitsexperten verwendet wird, um Schwachstellen in EC2-Instances zu erkennen, für die Patches erforderlich sind. Angreifer verwenden dieses Tool auch, um Schwachstellen in der EC2-Konfiguration zu finden und sich unbefugten Zugriff auf Ihre AWS Umgebung zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

PenTest:S3/ParrotLinux

Eine S3-API wurde von einem Computer mit Parrot Security Linux aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass ein Computer, auf dem Parrot Security Linux ausgeführt wird, S3-API-Aufrufe mit Anmeldeinformationen durchführt, die zu Ihrem AWS Konto gehören. Ihre Anmeldeinformationen wurden möglicherweise kompromittiert. Parrot Security Linux ist ein beliebtes Tool für Penetrationstests, das von Sicherheitsexperten verwendet wird, um Schwachstellen in

EC2-Instances zu erkennen, für die Patches erforderlich sind. Dieses Tool wird allerdings auch von Angreifern verwendet, um Schwächen in der EC2-Konfiguration zu finden und nicht autorisierten Zugriff auf Ihre AWS -Umgebung zu erhalten.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

PenTest:S3/PentooLinux

Eine S3-API wurde von einem Pentoo-Linux-Computer aus aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass ein Computer, auf dem Pentoo Linux ausgeführt wird, S3-API-Aufrufe mit Anmeldeinformationen durchführt, die zu Ihrem AWS Konto gehören. Ihre Anmeldeinformationen wurden möglicherweise kompromittiert. Pentoo Linux ist ein beliebtes Tool für Penetrationstests, das von Sicherheitsexperten verwendet wird, um Schwachstellen in EC2-Instances zu erkennen, für die Patches erforderlich sind. Angreifer verwenden dieses Tool auch, um Schwachstellen in der EC2-Konfiguration zu finden und sich unbefugten Zugriff auf Ihre AWS Umgebung zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Policy:S3/AccountBlockPublicAccessDisabled

Eine IAM-Entität hat eine API aufgerufen, die verwendet wird, um Amazon S3 Block Public Access auf einen Bucket zu deaktivieren.

Standard-Schweregrad: Niedrig

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie darüber, dass Amazon S3 Block Public Access auf Kontoebene deaktiviert wurde. Wenn S3 Block Public Access aktiviert ist, werden entsprechende Einstellungen verwendet, um die auf den Bucket angewendeten Richtlinien oder Zugriffssteuerungslisten (ACL) zu filtern, um eine unbeabsichtigte öffentliche Offenlegung von Daten zu verhindern.

In der Regel ist S3 Block Public Access deaktiviert, um den öffentlichen Zugriff auf einen Bucket oder die Objekte im Bucket zuzulassen. Wenn S3 Block Public Access für ein Konto deaktiviert ist, wird der Zugriff auf Ihre Buckets durch die Richtlinien, ACLs oder Einstellungen von Block Public Access auf Bucket-Ebene gesteuert, die für Ihre individuellen Buckets gelten. Dies bedeutet nicht, dass der Bucket öffentlich freigegeben ist. Sie sollten die auf den Bucket angewendeten Berechtigungen jedoch überprüfen, um sicherzustellen, dass die passenden Zugangsebenen angewendet werden.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Policy:S3/BucketAnonymousAccessGranted

Ein IAM-Prinzipal hat den Zugriff auf einen S3-Bucket auf das Internet gewährt, indem er Bucket-Richtlinien oder ACLs geändert hat.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie darüber, dass der aufgelistete S3-Bucket im Internet öffentlich zugänglich gemacht wurde, weil eine IAM-Entität eine Bucket-Richtlinie oder ACL für diesen Bucket geändert hat. Nachdem eine Änderung an der Richtlinie oder der ACL erkannt wurde, ermittelt anhand Automated Reasoning auf Basis von Zelkova, ob der Bucket öffentlich zugänglich ist.

> **Note**
>
> Wenn die ACLs oder Bucket-Richtlinien eines Buckets so konfiguriert sind, dass sie explizit oder alles verweigern, spiegelt diese Erkenntnis möglicherweise nicht den aktuellen Status des Buckets wider. Diese Erkenntnis spiegelt nicht die Einstellungen für den öffentlichen Zugriff in S3, die möglicherweise für Ihren S3-Bucket aktiviert wurden, wider. In solchen Fällen wird der `effectivePermission`-Wert im Ergebnis als `UNKNOWN` markiert.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Policy:S3/BucketBlockPublicAccessDisabled

Ein IAM-Prinzipal hat eine API aufgerufen, die verwendet wird, um S3 Block Public Access auf einen Bucket zu deaktivieren.

Standard-Schweregrad: Niedrig

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie darüber, dass Block Public Access für den S3-Bucket deaktiviert wurde. Wenn S3 Block Public Access aktiviert ist, werden entsprechende Einstellungen verwendet, um die auf den Bucket angewendeten Richtlinien oder Zugriffssteuerungslisten (ACL) zu filtern, um eine unbeabsichtigte öffentliche Offenlegung von Daten zu verhindern.

In der Regel ist S3 Block Public Access deaktiviert, um den öffentlichen Zugriff auf einen Bucket oder die Objekte im Bucket zuzulassen. Wenn S3 Block Public Access für diesen Bucket deaktiviert ist, wird der Zugriff auf den Bucket durch Richtlinien oder ACLs, gesteuert, die auf den Bucket angewendet sind. Dies bedeutet nicht, dass der Bucket öffentlich freigegeben ist. Sie sollten die auf den Bucket angewendeten Richtlinien und ACLs jedoch überprüfen, um sicherzustellen, dass die passenden Berechtigungen angewendet werden.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Policy:S3/BucketPublicAccessGranted

Ein IAM-Prinzipal hat allen AWS Benutzern öffentlichen Zugriff auf einen S3-Bucket gewährt, indem er die Bucket-Richtlinien oder ACLs geändert hat.

Standard-Schweregrad: Hoch

- Datenquelle: Verwaltungsereignisse CloudTrail

Dieses Ergebnis informiert Sie darüber, dass der aufgelistete S3-Bucket allen authentifizierten AWS Benutzern öffentlich zugänglich gemacht wurde, weil eine IAM-Entität eine Bucket-Richtlinie oder ACL für diesen S3-Bucket geändert hat. Nachdem eine Änderung an der Richtlinie oder der ACL erkannt wurde, ermittelt anhand Automated Reasoning auf Basis von Zelkova, ob der Bucket öffentlich zugänglich ist.

> **Note**
>
> Wenn die ACLs oder Bucket-Richtlinien eines Buckets so konfiguriert sind, dass sie explizit oder alles verweigern, spiegelt diese Erkenntnis möglicherweise nicht den aktuellen Status des Buckets wider. Diese Erkenntnis spiegelt nicht die Einstellungen für den öffentlichen Zugriff in S3, die möglicherweise für Ihren S3-Bucket aktiviert wurden, wider. In solchen Fällen wird der `effectivePermission`-Wert im Ergebnis als `UNKNOWN` markiert.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Stealth:S3/ServerAccessLoggingDisabled

S3-Server-Zugriffsprotokollierung für einen Bucket wurde deaktiviert.

Standard-Schweregrad: Niedrig

- Datenquelle: Verwaltungsereignisse CloudTrail

Dieses Ergebnis informiert Sie darüber, dass die Protokollierung des S3-Serverzugriffs für einen Bucket in Ihrer AWS Umgebung deaktiviert ist. Wenn diese Option deaktiviert ist, werden keine Webanforderungsprotokolle für Versuche erstellt, auf den identifizierten S3-Bucket zuzugreifen. Aufrufe der S3-Management-API an den Bucket, z. B. DeleteBucket, werden jedoch weiterhin verfolgt. Wenn die S3-Datenereignisprotokollierung CloudTrail für diesen Bucket aktiviert ist, werden Webanfragen für Objekte innerhalb des Buckets weiterhin verfolgt. Das Deaktivieren der Protokollierung ist eine Methode, die häufig von nicht autorisierten Benutzern verwendet wird, um ihre Spuren zu verwischen. Weitere Informationen zu S3-Protokollen finden Sie unter S3-Serverzugriffsprotokollierung und Optionen für S3-Protokollierung.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

Eine S3-API wurde von einer IP-Adresse aufgerufen, die sich auf einer benutzerdefinierten Bedrohungsliste befindet.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass ein S3-API-Vorgang, z. B. `PutObject` oder`PutObjectAcl` , von einer IP-Adresse aufgerufen wurde, die auf einer von Ihnen

hochgeladenen Bedrohungsliste steht. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

UnauthorizedAccess:S3/TorIPCaller

Eine S3-API wurde von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass ein S3-API-Vorgang, wie zum Beispiel `PutObject` oder `PutObjectAcl`, von einer IP-Adresse eines Tor-Ausgangsknotens aus aufgerufen wurde. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dieser Befund kann auf einen unbefugten Zugriff auf Ihre AWS Ressourcen hinweisen, um die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Nicht mehr aktive Erkenntnistypen

Eine Erkenntnis ist eine Benachrichtigung, die Details zu einem von GuardDuty festgestellten potenziellen Sicherheitsrisiko enthält. Weitere Informationen über wichtige Änderungen an den GuardDuty-Ergebnistypen, einschließlich neu hinzugefügter oder nicht mehr aktiver Ergebnistypen, finden Sie unter Dokumentenverlauf für Amazon GuardDuty.

Die folgenden Erkenntnistypen wurden eingestellt und werden nicht mehr von GuardDuty generiert.

> **Important**
>
> Sie können nicht mehr aktive GuardDuty-Erkenntnistypen nicht reaktivieren.

Themen

Exfiltration:S3/ObjectRead.Unusual

Eine IAM-Entität hat eine S3-API auf verdächtige Weise aufgerufen.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

- Datenquelle: CloudTrail-Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass eine IAM-Entität in Ihrer AWS-Umgebung API-Aufrufe tätigt, die einen S3-Bucket betreffen und die sich von der festgelegten Grundlinie dieser Entität unterscheiden. Der in dieser Aktivität verwendete API-Aufruf steht im Zusammenhang mit der Exfiltrationsphase eines Angriffs, in der ein Angreifer versucht, Daten zu sammeln. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise hatte diese IAM-Entität noch nie zuvor diese Art von API aufgerufen, oder die API wurde von einem ungewöhnlichen Ort aus aufgerufen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Impact:S3/PermissionsModification.Unusual

Eine IAM-Entität hat eine API aufgerufen, um die Berechtigungen für eine oder mehrere S3-Ressourcen zu ändern.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis informiert Sie darüber, dass eine IAM-Entität API-Aufrufe durchführt, um die Berechtigungen für einen oder mehrere Buckets oder Objekte in Ihrer AWS-Umgebung zu ändern. Diese Aktion kann von einem Angreifer ausgeführt werden, um die Weitergabe von Informationen außerhalb des Kontos zu ermöglichen. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise hatte diese IAM-Entität noch nie zuvor diese Art von API aufgerufen, oder die API wurde von einem ungewöhnlichen Ort aus aufgerufen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Impact:S3/ObjectDelete.Unusual

Eine IAM-Entität rief eine API zum Löschen von Daten in einem S3-Bucket auf.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Dieses Ergebnis informiert Sie darüber, dass eine bestimmte IAM-Entität in Ihrer AWS-Umgebung API-Aufrufe durchführt, um Daten im aufgeführten S3-Bucket zu löschen, indem der Bucket selbst gelöscht wird. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise hatte diese IAM-Entität noch nie zuvor diese Art von API aufgerufen, oder die API wurde von einem ungewöhnlichen Ort aus aufgerufen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv

genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Discovery:S3/BucketEnumeration.Unusual

Eine IAM-Entität hat eine S3-API aufgerufen, um S3-Buckets in Ihrem Netzwerk zu erkennen.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis informiert Sie darüber, dass eine IAM-Entität eine S3-API aufgerufen hat, um S3-Buckets in Ihrer Umgebung zu erkennen, z. B. `ListBuckets`. Diese Art von Aktivität steht im Zusammenhang mit der Erkennungsphase eines Angriffs, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihre AWS-Umgebung für einen umfassenderen Angriff anfällig ist. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise hatte diese IAM-Entität noch nie zuvor diese Art von API aufgerufen, oder die API wurde von einem ungewöhnlichen Ort aus aufgerufen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Persistence:IAMUser/NetworkPermissions

Ein IAM-Entität hat eine API aufgerufen, die üblicherweise verwendet wird, um die Netzwerkzugriffsberechtigungen für Sicherheitsgruppen, Routen und ACLs in Ihrem AWS-Konto zu ändern.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis bedeutet, dass ein bestimmter Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle, oder Benutzer) in Ihrer AWS-Umgebung ein Verhalten zeigt, das von seinem normalen Verhalten abweicht. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Diese Erkenntnis wird ausgelöst, wenn Netzwerkkonfigurationseinstellungen unter verdächtigen Umständen geändert werden, z. B. wenn ein Prinzipal die `CreateSecurityGroup`-API aufruft, ohne dies jemals in der Vergangenheit getan zu haben. Angreifer versuchen häufig, Sicherheitsgruppen zu ändern, um bestimmten eingehenden Datenverkehr auf verschiedenen Ports zuzulassen und besser auf eine EC2-Instance zugreifen zu können.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Persistence:IAMUser/ResourcePermissions

Ein Prinzipal hat eine API aufgerufen, die üblicherweise verwendet wird, um Sicherheitszugriffsrichtlinien verschiedener Ressourcen in Ihrem AWS-Konto zu ändern.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis bedeutet, dass ein bestimmter Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle, oder Benutzer) in Ihrer AWS-Umgebung ein Verhalten zeigt, das von seinem normalen Verhalten abweicht. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Diese Erkenntnis wird ausgelöst, wenn eine Änderung an Richtlinien oder Berechtigungen festgestellt wird, die mit AWS-Ressourcen verknüpft sind, z. B. wenn ein Prinzipal in Ihrer AWS-Umgebung die `PutBucketPolicy` API aufruft, ohne dies je in der Vergangenheit getan zu haben. Einige Services, z. B. Amazon S3, unterstützen ressourcengebundene Berechtigungen, die einem oder mehreren Prinzipalen Zugriff auf die Ressource gewähren. Mit gestohlenen Anmeldeinformationen können Angreifer die einer Ressource zugeordneten Richtlinien ändern, um sich künftig Zugriff auf diese Ressource zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Persistence:IAMUser/UserPermissions

Ein Prinzipal hat eine API aufgerufen, die üblicherweise dazu verwendet wird, IAM-Benutzer, Gruppen oder Richtlinien in Ihrem AWS-Konto hinzuzufügen, zu ändern oder zu löschen.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis bedeutet, dass ein bestimmter Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle, oder Benutzer) in Ihrer AWS-Umgebung ein Verhalten zeigt, das von seinem normalen Verhalten abweicht. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Diese Erkenntnis wird durch verdächtige Änderungen an den benutzerbezogenen Berechtigungen in Ihrer AWS Umgebung ausgelöst, z. B. wenn ein Principal in Ihrer AWS-Umgebung die

`AttachUserPolicy`-API aufruft, ohne dies je in der Vergangenheit getan zu haben. Angreifer können gestohlene Anmeldeinformationen verwenden, um neue Benutzer zu erstellen, Zugriffsrichtlinien für bestehende Benutzer hinzuzufügen oder Zugriffsschlüssel zu erstellen, um ihren Zugriff auf ein Konto zu maximieren, selbst wenn ihr ursprünglicher Zugangspunkt geschlossen ist. Beispielsweise könnte der Besitzer des Kontos feststellen, dass ein bestimmter IAM-Benutzer oder ein bestimmtes IAM-Passwort gestohlen wurde, und es aus dem Konto löschen. Andere Benutzer, die von einem betrügerisch erstellten Administratorprinzipal erstellt wurden, werden jedoch möglicherweise nicht gelöscht, sodass der Angreifer auf ihr AWS-Konto zugreifen kann.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

PrivilegeEscalation:IAMUser/AdministrativePermissions

Ein Prinzipal hat versucht, sich selbst eine hochgradig weitreichende Richtlinie zuzuweisen.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Wenn der Angriff auf die Berechtigungseskalation nicht erfolgreich war, ist der Schweregrad des Ergebnises „Niedrig“, wenn der Angriff erfolgreich war, ist der Schweregrad „Mittel“.

Diese Erkenntnis informiert Sie darüber, dass ein bestimmter IAM-Entität in Ihrer AWS-Umgebung ein Verhalten zeigt, das auf einen ein Rechteeskalationsangriff hinweist. Diese Erkenntnis wird ausgelöst, wenn ein IAM-Benutzer oder eine Rolle versucht, sich selbst eine hochgradig weitreichende Richtlinie zuzuweisen. Wenn der/die entsprechende Benutzer oder Rolle nicht über administrative Rechte verfügen darf, können entweder die Anmeldeinformationen des Benutzers kompromittiert sein oder die Berechtigungen der Rolle wurden nicht ordnungsgemäß konfiguriert.

Angreifer können gestohlene Anmeldeinformationen verwenden, um neue Benutzer zu erstellen, Zugriffsrichtlinien für bestehende Benutzer hinzuzufügen oder Zugriffsschlüssel zu erstellen, um ihren Zugriff auf ein Konto zu maximieren, selbst wenn ihr ursprünglicher Zugangspunkt geschlossen ist. Der Eigentümer des Kontos stellt möglicherweise fest, dass ein bestimmter IAM-Benutzer

oder ein Passwort gestohlen wurden, und löscht diese aus dem Konto. Hierbei entfernt er aber möglicherweise andere Benutzer nicht, die vom betrügerisch angelegten Admin-Prinzipal angelegt wurden, sodass ihr AWS-Konto dem Angreifer weiterhin zur Verfügung steht.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Recon:IAMUser/NetworkPermissions

Ein Prinzipal hat eine API aufgerufen, die üblicherweise verwendet wird, um die Netzwerkzugriffsberechtigungen für Sicherheitsgruppen, Routen und ACLs in Ihrem AWS-Konto zu ändern.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis bedeutet, dass ein bestimmter Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle, oder Benutzer) in Ihrer AWS-Umgebung ein Verhalten zeigt, das von seinem normalen Verhalten abweicht. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Diese Erkenntnis wird ausgelöst, wenn Ressourcen-Zugriffsberechtigungen in Ihrem AWS-Konto unter fragwürdigen Umständen untersucht werden. Dies trifft beispielsweise dann zu, wenn ein Prinzipal zum ersten Mal die `DescribeInstances`-API aufgerufen hat. Ein Angreifer könnte gestohlene Anmeldeinformationen verwenden, um in Kenntnis Ihrer AWS-Ressourcen zu gelangen, um wertvolle Informationen herauszufinden oder festzustellen, welcher Funktionsumfang den Anmeldeinformationen bereits zur Verfügung steht.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Recon:IAMUser/ResourcePermissions

Ein Prinzipal hat eine API aufgerufen, die üblicherweise verwendet wird, um Sicherheitszugriffsrichtlinien verschiedener Ressourcen in Ihrem AWS-Konto zu ändern.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis bedeutet, dass ein bestimmter Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle, oder Benutzer) in Ihrer AWS-Umgebung ein Verhalten zeigt, das von seinem normalen Verhalten abweicht. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Diese Erkenntnis wird ausgelöst, wenn Ressourcen-Zugriffsberechtigungen in Ihrem AWS-Konto unter fragwürdigen Umständen untersucht werden. Dies trifft beispielsweise dann zu, wenn ein Prinzipal zum ersten Mal die `DescribeInstances`-API aufgerufen hat. Ein Angreifer könnte gestohlene Anmeldeinformationen verwenden, um in Kenntnis Ihrer AWS-Ressourcen zu gelangen, um wertvolle Informationen herauszufinden oder festzustellen, welcher Funktionsumfang den Anmeldeinformationen bereits zur Verfügung steht.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Recon:IAMUser/UserPermissions

Ein Prinzipal hat eine API aufgerufen, die üblicherweise dazu verwendet wird, IAM-Benutzer, Gruppen oder Richtlinien in Ihrem AWS-Konto hinzuzufügen, zu ändern oder zu löschen.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis wird ausgelöst, wenn Benutzerberechtigungen in Ihrer AWS-Umgebung unter fragwürdigen Umständen untersucht werden. Dies trifft beispielsweise dann zu, wenn ein Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle, oder Benutzer) zum ersten Mal die `ListInstanceProfilesForRole`-API aufgerufen hat. Ein Angreifer könnte gestohlene Anmeldeinformationen verwenden, um in Kenntnis Ihrer AWS-Ressourcen zu gelangen, um wertvolle Informationen herauszufinden oder festzustellen, welcher Funktionsumfang den Anmeldeinformationen bereits zur Verfügung steht.

Diese Erkenntnis zeigt an, dass ein bestimmter Prinzipal in der AWS-Umgebung ein Verhalten zeigt, das von seinem normalen Verhalten abweicht. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

ResourceConsumption:IAMUser/ComputeResources

Ein Prinzipal hat eine API aufgerufen, die häufig zum Starten von Datenverarbeitungsressourcen verwendet wird, wie beispielsweise EC2-Instances.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis wird ausgelöst, wenn EC2-Instances im aufgeführten Konto in Ihrer AWS-Umgebung unter fragwürdigen Umständen gestartet werden. Diese Erkenntnis deutet darauf hin, dass ein bestimmter Prinzipal in Ihrer AWS-Umgebung ein Verhalten zeigt, das von der etablierten Grundlinie abweicht, z. B. wenn ein Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle oder IAM-Benutzer) die `RunInstances`-API aufruft, ohne dies zuvor jemals getan zu haben. Dies kann ein Anzeichen für ein Angreifer sein, der gestohlene Anmeldeinformationen nutzt, um Rechenzeit zu stehlen (beispielsweise für das Mining von Kryptowährung, oder zum Entschlüsseln von Passwörtern). Es kann auch ein Hinweis auf einen Angreifer sein, der eine EC2-Instance in Ihrer AWS-Umgebung und ihre Anmeldeinformationen nutzt, um auf Ihr Konto zuzugreifen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Stealth:IAMUser/LoggingConfigurationModified

Ein Prinzipal hat eine API aufgerufen, die üblicherweise verwendet wird, um die CloudTrail-Protokollierung zu beenden, vorhandene Protokolle zu löschen und anderweitig Aktivitätsspuren aus Ihrem AWS-Konto zu entfernen.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis wird ausgelöst, wenn die Protokollierungskonfiguration in dem aufgeführten AWS-Konto in Ihrer Umgebung unter fragwürdigen Umständen geändert wird. Diese Erkenntnis deutet darauf hin, dass ein bestimmter Prinzipal in Ihrer AWS-Umgebung ein Verhalten zeigt, das von der etablierten Grundlinie abweicht, z. B. wenn ein Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle oder IAM-Benutzer) die `StopLogging`-API aufruft, ohne dies zuvor jemals getan zu haben. Dies kann darauf hinweisen, dass ein Angreifer versucht, seine Spuren zu verwischen, indem er alle Anzeichen von Aktivität entfernt.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

UnauthorizedAccess:IAMUser/ConsoleLogin

In Ihrem AWS-Konto wurde eine ungewöhnliche Konsolen-Anmeldung durch einen Prinzipal festgestellt.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Dieses Ergebnis wird ausgelöst, wenn eine Konsolenanmeldung unter fragwürdigen Umständen erkannt wird. Dies ist beispielsweise dann der Fall, wenn ein Prinzipal die ConsoleLogin-API zum ersten Mal von einem nie zuvor verwendeten Client oder von einem ungewöhnlichen Standort aus aufgerufen hat. Dies könnte darauf hinweisen, dass gestohlene Anmeldeinformationen verwendet werden, um Zugriff auf Ihr AWS-Konto zu erlangen, oder dass ein gültiger Benutzer auf ungültige oder wenig sichere Weise auf das Konto zugreift (z. B. nicht über ein zugelassenes VPN).

Diese Erkenntnis informiert Sie darüber, dass ein bestimmter Prinzipal in der AWS-Umgebung ein Verhalten zeigt, das von seinem normalen Verhalten abweicht. Für diesen Prinzipal gibt es keinen vorherigen Verlauf von Anmeldeaktivitäten mit dieser Client-Anwendung von diesem bestimmten Standort aus.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

UnauthorizedAccess:EC2/TorIPCaller

Ihre EC2-Instance erhält eingehende Verbindungen von einem Tor-Exit-Knoten.

Standard-Schweregrad: Mittel

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung eingehende Verbindungen von einem Tor-Ausgangsknotens erhält. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Diese Erkenntnis kann auf einen unbefugten Zugriff auf die AWS-Ressourcen hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Backdoor:EC2/XORDDOS

Eine EC2-Instance versucht, mit einer IP-Adresse zu kommunizieren, die mit XOR-DDoS-Malware in Verbindung steht.

Standard-Schweregrad: Hoch

Diese Erkenntnis informiert Sie, dass eine EC2-Instance in der AWS-Umgebung versucht, mit einer IP-Adresse zu kommunizieren, die mit XOR-DDoS-Malware in Verbindung steht. Diese EC2-Instance wurde möglicherweise kompromittiert. XOR DDoS ist eine Trojaner-Malware, die Linux-Systeme kapert. Um Zugriff auf das System zu erhalten, startet sie einen Brute-Force-Angriff, um das Passwort für Secure Shell (SSH)-Services auf Linux zu ermitteln. Nachdem die SSH-Anmeldeinformationen erlangt wurden und die Anmeldung erfolgreich war, wird ein Skript mit Root-Berechtigungen ausgeführt, um XOR DDoS herunterzuladen und zu installieren. Diese Malware wird dann als Teil eines Botnets verwendet, um verteilte DDoS-Angriffe (Distributed Denial-of-Service) auf andere Ziele zu durchzuführen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

Behavior:IAMUser/InstanceLaunchUnusual

Ein Benutzer hat eine EC2-Instance eines ungewöhnlichen Typs gestartet.

Standard-Schweregrad: Hoch

Diese Erkenntnis informiert Sie, dass ein bestimmter Benutzer in Ihrer AWS-Umgebung ein Verhalten zeigt, das sich von seinem normalen Verhalten unterscheidet. Dieser Benutzer hat bisher keine EC2-Instance dieses Typs gestartet. Ihre Anmeldeinformationen wurden möglicherweise kompromittiert.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

CryptoCurrency:EC2/BitcoinTool.A

Eine EC2-Instance kommuniziert mit Bitcoin-Mining-Pools.

Standard-Schweregrad: Hoch

Diese Erkenntnis informiert Sie, dass eine EC2-Instance in Ihrer AWS-Umgebung mit Bitcoin-Mining-Pools kommuniziert. Beim Mining von Kryptowährungen werden Ressourcen in einem Pool kombiniert, damit die Verarbeitungsleistung über ein Netzwerk gemeinsam genutzt werden kann. Der Gewinn wird dann nach Maßgabe der zur Lösung des Blocks beigetragenen Arbeit aufgeteilt. Wenn Sie diese EC2-Instance nicht für Bitcoin-Mining verwenden, könnte Ihre EC2-Instance kompromittiert worden sein.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

UnauthorizedAccess:IAMUser/UnusualASNCaller

Eine API wurde von einer IP-Adresse eines unüblichen Netzwerks aufgerufen.

Standard-Schweregrad: Hoch

Dieses Ergebnis informiert Sie darüber, dass eine bestimmte Aktivität von einer IP-Adresse eines unüblichen Netzwerks aufgerufen wurde. Dieses Netzwerk wurde im gesamten AWS-Nutzungsverlauf des beschriebenen Benutzers noch nie beobachtet. Diese Aktivität kann eine Konsolen-Anmeldung, einen Versuch, eine EC2-Instance zu starten, einen neuen IAM-Benutzer anzulegen, Ihre AWS-Privilegien zu ändern usw. beinhalten. Dies kann auf einen unbefugten Zugriff auf Ihre AWS-Ressourcen hinweisen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.

Erkenntnisse nach Ressourcentyp

Die folgenden Seiten sind nach dem Ressourcentyp kategorisiert, der mit einem GuardDuty Ergebnis verknüpft ist:

- EC2-Erkenntnistypen
- Runtime Monitoring: Typen finden
- IAM-Erkenntnistypen
- EKS-Auditprotokolle zum Auffinden von Typen
- Lambda-Protection-Erkenntnistypen
- Erkenntnistypen für Malware Protection
- Erkenntnistypen für RDS Protection
- S3-Erkenntnistypen

Tabelle mit den Erkenntnissen

Die folgende Tabelle zeigt alle aktiven Erkenntnistypen, sortiert nach der zugrunde liegenden Datenquelle oder das jeweiligen Feature. Einige der folgenden Erkenntnistypen können einen unterschiedlichen Schweregrad haben, der durch ein Sternchen (*) gekennzeichnet ist. Informationen zum variablen Schweregrad eines Erkenntnistyps finden Sie in der detaillierten Beschreibung dieses Erkenntnistyps.

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Discovery:S3/AnomalousBehavior	Amazon S3	CloudTrail Datenereignisse für S3	Niedrig
Discovery:S3/MaliciousIPCaller	Amazon S3	CloudTrail Datenereignisse für S3	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Discovery:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Discovery:S3/TorIPCaller	Amazon S3	CloudTrail Datenereignisse für S3	Mittelschwer
Exfiltration:S3/AnomalousBehavior	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Exfiltration:S3/MaliciousIPCaller	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Impact:S3/AnomalousBehavior.Delete	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Impact:S3/AnomalousBehavior.Permission	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Impact:S3/AnomalousBehavior.Write	Amazon S3	CloudTrail Datenereignisse für S3	Mittelschwer
Impact:S3/MaliciousIPCaller	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
PenTest:S3/KaliLinux	Amazon S3	CloudTrail Datenereignisse für S3	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
PenTest:S3/ParrotLinux	Amazon S3	CloudTrail Datenereignisse für S3	Mittelschwer
PenTest:S3/PentooLinux	Amazon S3	CloudTrail Datenereignisse für S3	Mittelschwer
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Ereignis	Mittelschwer
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Veranstaltung	Niedrig
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Veranstaltung	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Veranstaltung	Hoch
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
PenTest:IAMUser/KaliLinux	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
PenTest:IAMUser/ParrotLinux	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
PenTest:IAMUser/PentooLinux	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
Persistence:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
Stealth:IAMUser/PasswordPolicyChange	IAM	CloudTrail Management-Veranstaltung	Niedrig*

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	IAM	CloudTrail Management-Veranstaltung	Hoch*
Policy:S3/AccountBlockPublicAccessDisabled	Amazon S3	CloudTrail Management-Veranstaltung	Niedrig
Policy:S3/BucketAnonymousAccessGranted	Amazon S3	CloudTrail Management-Veranstaltung	Hoch
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	CloudTrail Management-Veranstaltung	Niedrig
Policy:S3/BucketPublicAccessGranted	Amazon S3	CloudTrail Management-Veranstaltung	Hoch
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Veranstaltung	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
Recon:IAMUser/TorIPCaller	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail Management-Veranstaltung	Niedrig
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	CloudTrail Management-Veranstaltung	Niedrig
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail Management-Veranstaltung	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail Verwaltungsereignisse oder CloudTrail Datenereignisse für S3	Niedrig
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail Verwaltungsereignisse oder CloudTrail Datenereignisse für S3	Hoch
Backdoor:EC2/C&CActivity.B!DNS	Amazon EC2	DNS-Protokolle	Hoch
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	DNS-Protokolle	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	DNS-Protokolle	Mittelschwer
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	DNS-Protokolle	Hoch
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	DNS-Protokolle	Hoch
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	DNS-Protokolle	Niedrig
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	DNS-Protokolle	Mittelschwer
Trojan:EC2/DGADomainRequest.B	Amazon EC2	DNS-Protokolle	Hoch
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	DNS-Protokolle	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Trojan:EC2/DNSDataExfiltration	Amazon EC2	DNS-Protokolle	Hoch
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	DNS-Protokolle	Hoch
Trojan:EC2/DropPoint!DNS	Amazon EC2	DNS-Protokolle	Mittelschwer
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	DNS-Protokolle	Hoch
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	DNS-Protokolle	Hoch
Execution:Container/MaliciousFile	Container	EBS-Malware-Schutz	Variiert je nach erkannter Bedrohung
Execution:Container/SuspiciousFile	Container	EBS-Malware-Schutz	Variiert je nach erkannter Bedrohung
Execution:EC2/MaliciousFile	EC2	EBS-Malware-Schutz	Variiert je nach erkannter Bedrohung

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Execution:EC2/SuspiciousFile	EC2	EBS-Malware-Schutz	Variiert je nach erkannter Bedrohung
Execution:ECS/MaliciousFile	ECS	EBS-Malware-Schutz	Variiert je nach erkannter Bedrohung
Execution:ECS/SuspiciousFile	ECS	EBS-Malware-Schutz	Variiert je nach erkannter Bedrohung
Execution:Kubernetes/MaliciousFile	Kubernetes	EBS-Malware-Schutz	Variiert je nach erkannter Bedrohung
Execution:Kubernetes/SuspiciousFile	Kubernetes	EBS-Malware-Schutz	Variiert je nach erkannter Bedrohung
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	EKS-Auditprotokolle	Mittelschwer
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	EKS-Auditprotokolle	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS-Auditprotokolle	Hoch
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS-Auditprotokolle	Hoch
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	EKS-Auditprotokolle	Hoch
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	EKS-Auditprotokolle	Hoch
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS-Auditprotokolle	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS-Auditprotokolle	Hoch
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	EKS-Auditprotokolle	Hoch
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	EKS-Auditprotokolle	Niedrig
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	EKS-Auditprotokolle	Mittelschwer
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS-Auditprotokolle	Mittelschwer
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS-Auditprotokolle	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Discovery:Kubernetes/TorIPCaller	Kubernetes	EKS-Auditprotokolle	Mittelschwer
Execution:Kubernetes/ExecInKubeSystemPod	Kubernetes	EKS-Auditprotokolle	Mittelschwer
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	EKS-Auditprotokolle	Mittelschwer
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	EKS-Auditprotokolle	Niedrig
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	EKS-Auditprotokolle	Hoch
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS-Auditprotokolle	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS-Auditprotokolle	Hoch
Impact:Kubernetes/TorIPCaller	Kubernetes	EKS-Auditprotokolle	Hoch
Persistence:Kubernetes/ContainerWithSensitiveMount	Kubernetes	EKS-Auditprotokolle	Mittelschwer
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	EKS-Auditprotokolle	Mittelschwer
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS-Auditprotokolle	Mittelschwer
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS-Auditprotokolle	Hoch
Persistence:Kubernetes/TorIPCaller	Kubernetes	EKS-Auditprotokolle	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	EKS-Auditprotokolle	Hoch
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	EKS-Auditprotokolle	Hoch
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	EKS-Auditprotokolle	Mittelschwer
Policy:Kubernetes/ExposedDashboard	Kubernetes	EKS-Auditprotokolle	Mittelschwer
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	Kubernetes	EKS-Auditprotokolle	Mittel*

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	Kubernetes	EKS-Auditprotokolle	Niedrig
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	EKS-Auditprotokolle	Hoch
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	EKS-Auditprotokolle	Hoch
PrivilegeEscalation:Kubernetes/PrivilegedContainer	Kubernetes	EKS-Auditprotokolle	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Backdoor:Lambda/C&CActivity.B	Lambda	Lambda Network Activity Monitoring	Hoch
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Lambda Network Activity Monitoring	Hoch
Trojan:Lambda/BlackholeTraffic	Lambda	Lambda Network Activity Monitoring	Mittelschwer
Trojan:Lambda/DropPoint	Lambda	Lambda Network Activity Monitoring	Mittelschwer
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Lambda Network Activity Monitoring	Mittelschwer
UnauthorizedAccess:Lambda/TorClient	Lambda	Lambda Network Activity Monitoring	Hoch
UnauthorizedAccess:Lambda/TorRelay	Lambda	Lambda Network Activity Monitoring	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	Unterstützte Amazon-Aurora-Datenbanken	RDS Login Activity Monitoring	Niedrig
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	Unterstützte Amazon-Aurora-Datenbanken	RDS Login Activity Monitoring	Hoch
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	Unterstützte Amazon-Aurora-Datenbanken	RDS Login Activity Monitoring	Variable*
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	Unterstützte Amazon-Aurora-Datenbanken	RDS Login Activity Monitoring	Mittelschwer
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	Unterstützte Amazon-Aurora-Datenbanken	RDS Login Activity Monitoring	Hoch
CredentialAccess:RDS/TorIPCaller.FailedLogin	Unterstützte Amazon-Aurora-Datenbanken	RDS Login Activity Monitoring	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	Unterstützte Amazon-Aurora-Datenbanken	RDS Login Activity Monitoring	Hoch
Discovery:RDS/MaliciousIPCaller	Unterstützte Amazon-Aurora-Datenbanken	RDS Login Activity Monitoring	Mittelschwer
Discovery:RDS/TorIPCaller	Unterstützte Amazon-Aurora-Datenbanken	RDS Login Activity Monitoring	Mittelschwer
Backdoor:Runtime/C&CActivity.B	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch
Backdoor:Runtime/C&CActivity.B!DNS	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch
CryptoCurrency:Runtime/BitcoinTool.B	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch
CryptoCurrency:Runtime/BitcoinTool.B!DNS	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
DefenseEvasion:Runtime/FilelessExecution	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
DefenseEvasion:Runtime/ProcessInjection.Proc	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch
DefenseEvasion:Runtime/ProcessInjection.Ptrace	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch
DefenseEvasion:Runtime/PtraceAntiDebugging	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Niedrig
DefenseEvasion:Runtime/SuspiciousCommand	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch
Execution:Runtime/MaliciousFileExecuted	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Execution:Runtime/NewBinaryExecuted	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Execution:Runtime/NewLibraryLoaded	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Execution:Runtime/SuspiciousCommand	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Variable
Execution:Runtime/SuspiciousTool	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Variable
Execution:Runtime/ReverseShell	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch
Impact:Runtime/AbusedDomainRequest.Reputation	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Impact:Runtime/BitcoinDomainRequest.Reputation	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch
Impact:Runtime/CryptoMinerExecuted	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch
Impact:Runtime/MaliciousDomainRequest.Reputation	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Impact:Runtime/SuspiciousDomainRequest.Reputation	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Niedrig
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Privilege Escalation:Runtime/ContainerMountsHostDirectory	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Privilege Escalation:Runtime/DockerSocketAccessed	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Privilege Escalation:Runtime/RuncContainerEscape	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch
Privilege Escalation:Runtime/UserfaultfdUsage	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Trojan:Runtime/BlackholeTraffic	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Trojan:Runtime/BlackholeTraffic!DNS	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Trojan:Runtime/DropPoint	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Trojan:Runtime/DGADomainRequest.C!DNS	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch
Trojan:Runtime/DriveBySourceTraffic!DNS	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch
Trojan:Runtime/DropPoint!DNS	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Trojan:Runtime/PhishingDomainRequest!DNS	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch
UnauthorizedAccess:Runtime/MetadataDNSRebind	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch
UnauthorizedAccess:Runtime/TorClient	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
UnauthorizedAccess:Runtime/TorRelay	Instanz, EKS-Cluster, ECS-Cluster oder Container	Laufzeit-Überwachung	Hoch
Backdoor:EC2/C&CActivity.B	EC2	VPC Flow Logs	Hoch
Backdoor:EC2/DenialOfService.Dns	EC2	VPC Flow Logs	Hoch
Backdoor:EC2/DenialOfService.Tcp	EC2	VPC Flow Logs	Hoch
Backdoor:EC2/DenialOfService.Udp	EC2	VPC Flow Logs	Hoch
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	EC2	VPC Flow Logs	Hoch
Backdoor:EC2/DenialOfService.UnusualProtocol	EC2	VPC Flow Logs	Hoch
Backdoor:EC2/Spambot	EC2	VPC Flow Logs	Mittelschwer
Behavior:EC2/NetworkPortUnusual	EC2	VPC Flow Logs	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Behavior:EC2/TrafficVolumeUnusual	EC2	VPC Flow Logs	Mittelschwer
CryptoCurrency:EC2/BitcoinTool.B	EC2	VPC Flow Logs	Hoch
DefenseEvasion:EC2/UnusualDNSResolver	EC2	VPC Flow Logs	Mittelschwer
DefenseEvasion:EC2/UnusualDoHActivity	EC2	VPC Flow Logs	Mittelschwer
DefenseEvasion:EC2/UnusualDoTActivity	EC2	VPC Flow Logs	Mittelschwer
Impact:EC2/PortSweep	EC2	VPC Flow Logs	Hoch
Impact:EC2/WinRMBruteForce	EC2	VPC Flow Logs	Niedrig*
Recon:EC2/PortProbeEMRUnprotectedPort	EC2	VPC Flow Logs	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Recon:EC2/PortProbeUnprotectedPort	EC2	VPC Flow Logs	Niedrig*
Recon:EC2/Portscan	EC2	VPC Flow Logs	Mittelschwer
Trojan:EC2/BlackholeTraffic	EC2	VPC Flow Logs	Mittelschwer
Trojan:EC2/DropPoint	EC2	VPC Flow Logs	Mittelschwer
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	EC2	VPC Flow Logs	Mittelschwer
UnauthorizedAccess:EC2/RDPBruteForce	EC2	VPC Flow Logs	Niedrig*
UnauthorizedAccess:EC2/SSHBruteForce	EC2	VPC Flow Logs	Niedrig*
UnauthorizedAccess:EC2/TorClient	EC2	VPC Flow Logs	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
UnauthorizedAccess:EC2/TorRelay	EC2	VPC Flow Logs	Hoch

Verwaltung der GuardDuty Amazon-Ergebnisse

GuardDuty bietet mehrere wichtige Funktionen, mit denen Sie Ihre Ergebnisse sortieren, speichern und verwalten können. Mit diesen Funktionen können Sie Erkenntnisse an Ihre spezifische Umgebung anpassen. Dadurch können Sie erkenntnisbedingtes Rauschen niedrigen Schweregrads reduzieren und sich auf spezifische Bedrohungen für Ihre AWS -Umgebung konzentrieren. Lesen Sie sich die Themen auf dieser Seite durch, um zu erfahren, wie Sie diese Funktionen nutzen können, um den Wert Ihrer GuardDuty Ergebnisse zu steigern.

Themen:

verdächtige Aktivitäten in Ihrem Konto nachzuverfolgen und zu bewerten, ob die empfohlenen Abhilfemaßnahmen erfolgreich waren.

Erstellen von benutzerdefinierten Antworten auf GuardDuty Erkenntnisse mit Amazon CloudWatch Events

Richten Sie automatische Benachrichtigungen für GuardDuty Ergebnisse im Rahmen von CloudWatch Amazon-Veranstaltungen ein. Sie können auch andere Aufgaben mithilfe von CloudWatch Events automatisieren, um auf Ergebnisse zu reagieren.

Grundlegendes zu CloudWatch Protokollen und Gründen für das Überspringen von Ressourcen beim Malware-Schutz-Scan

Erfahren Sie, wie Sie die CloudWatch Logs for GuardDuty Malware Protection überprüfen können und aus welchen Gründen Ihre betroffenen Amazon EC2 EC2-Instance- oder Amazon EBS-Volumes während des Scanvorgangs möglicherweise übersprungen wurden.

Falschmeldungen in GuardDuty Malware Protection melden

Erfahren Sie mehr über die falsch positiven Erfahrungen mit GuardDuty Malware Protection und wie Sie falsch positive Bedrohungserkennungen melden können.

Übersichts-Dashboard

Das Übersichts-Dashboard bietet eine aggregierte Ansicht der GuardDuty Ergebnisse, die AWS-Konto in Ihrer aktuellen Region generiert wurden. Derzeit unterstützt das Dashboard ein Volumen von bis zu 5 000 Erkenntnissen. Sie können jedoch die Details aller Ergebnisse einsehen, indem Sie entweder die Ergebnisseite in der GuardDuty Konsole oder oder GetFindingsoder ListFindingsverwenden.

> **Note**
>
> Die Zusammenfassung der Ergebnisse ist nur über die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/ verfügbar.

Die folgenden Abschnitten helfen Ihnen, auf das Dashboard zuzugreifen und dessen Komponenten zu verstehen.

Inhalt

Zugriff auf das Zusammenfassungs-Dashboard

Auf der GuardDuty Konsole zeigt das Übersichts-Dashboard eine konsolidierte Ansicht der letzten 5.000 GuardDuty Ergebnisse, die in der aktuellen Region generiert wurden.

So greifen Sie auf das Zusammenfassungs-Dashboard zu

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Zusammenfassung aus. Wenn Sie die Konsole öffnen, GuardDuty wird das Übersichts-Dashboard angezeigt.
3. Standardmäßig wird die Zusammenfassung für denselben Tag angezeigt – Heute. Die GuardDuty Konsole bietet eine Option zum Anzeigen der Zusammenfassung der letzten 2 Tage, der letzten 7 Tage und der letzten 30 Tage. Um den Standardzeitbereich zu ändern, wählen Sie eine der Optionen aus dem Drop-down-Menü über dem Übersichtsbereich.
4. Filtern der Daten

   - Die Widgets Konten mit den meisten Erkenntnissen, Ressourcen mit den meisten Erkenntnissen und Am wenigsten vorkommende Erkenntnisse können die Daten nach dem Schweregrad der Ergebnisse filtern.
   - Das Widget Ressourcen mit den meisten Erkenntnissen hilft Ihnen auch dabei, die Daten auf der Grundlage Ihres potenziell betroffenen Ressourcentyps zu filtern.

     Ein Mitgliedskonto kann die Details der potenziell betroffenen Ressource einsehen, die zu seinem eigenen Konto gehört. Wenn Sie ein GuardDuty Administratorkonto haben und die Details der potenziell betroffenen Ressource einsehen möchten, öffnen Sie die GuardDuty Konsole mit den Anmeldeinformationen des zugehörigen Mitgliedskontos.
5. Geltungsbereich der Schutzpläne

   Der Geltungsbereich der Schutzpläne gibt die Anzahl der Mitgliedskonten an, die GuardDuty in Ihrer Organisation aktiviert wurden. Die Statistiken sind nur für den delegierten GuardDuty Administrator sichtbar.

Verstehen des Zusammenfassungs-Dashboards

Das Zusammenfassungs-Dashboard zeigt die aggregierten Daten in den folgenden Abschnitten. Bevor Sie sich die Zusammenfassung ansehen und verstehen, stellen Sie sicher, dass Sie in der Regionsauswahl oben in der Konsole die gewünschte AWS-Region auswählen. Stellen Sie außerdem sicher, dass Sie den gewünschten Zeitraum aus dem Dropdownmenü über dem Übersichtsbereich auswählen. Wenn für die ausgewählten Parameter keine Erkenntnisse generiert wurden, sind in keinem der Widgets Daten verfügbar.

Aus einer Menge von bis zu 5.000 GuardDuty Ergebnissen werden im Übersichts-Dashboard mit den Konten mit den meisten Ergebnissen, Ressourcen mit den meisten Ergebnissen und den am wenigsten vorkommenden Ergebnissen die Daten angezeigt, die auf den fünf wichtigsten Ergebnissen basieren. Eine eingehendere Analyse finden Sie auf der Ergebnisseite in der GuardDuty Konsole.

Übersicht

Diese Einstellung bietet die folgenden Optionen:

- Erkenntnisse insgesamt: Gibt die Gesamtzahl von Erkenntnissen an, die in Ihrem Konto in der aktuellen Region generiert wurden.
- Ergebnisse mit hohem Schweregrad: Gibt die Anzahl der GuardDuty Ergebnisse an, die in der aktuellen Region einen hohen Schweregrad aufweisen.
- Ressourcen mit Erkenntnissen: Gibt die Anzahl der Ressourcen an, die mit einer Erkenntnis verknüpft sind und möglicherweise gefährdet wurden.
- Konten mit Erkenntnissen: Gibt die Anzahl der Konten an, in denen mindestens eine Erkenntnis generiert wurde. Wenn Sie ein eigenständiges Konto haben, ist der Wert in diesem Feld 1.

Für die Zeitbereiche Letzte 7 Tage und Letzte 30 Tage kann im Bereich Übersicht der prozentuale Unterschied zwischen den generierten Erkenntnissen von Woche zu Woche (WoW) bzw. Monat zu Monat (MoM) angezeigt werden. Wenn in der Woche oder im Monat zuvor keine Erkenntnisse generiert wurden und keine Vergleichsdaten vorliegen, ist die prozentuale Differenz möglicherweise nicht verfügbar.

Wenn Sie ein GuardDuty Administratorkonto haben, enthalten all diese Felder die zusammengefassten Daten aller Mitgliedskonten in Ihrer Organisation.

Erkenntnisse nach Schweregrad

In diesem Abschnitt wird ein Balkendiagramm mit der Gesamtzahl der Erkenntnisse im ausgewählten Zeitraum angezeigt. Sie können die Anzahl der Erkenntnisse mit niedrigem, mittlerem oder hohem Schweregrad anzeigen, die an einem bestimmten Datum innerhalb des ausgewählten Zeitraums generiert wurden.

Die häufigsten Arten von Erkenntnissen

In diesem Abschnitt werden die fünf häufigsten Ergebnisarten anhand eines Kreisdiagramms anhand einer Menge von bis zu 5.000 GuardDuty Ergebnissen dargestellt, die in der aktuellen Region generiert wurden. In diesem Kreisdiagramm werden die folgenden Daten angezeigt, wenn Sie den Mauszeiger über die einzelnen Sektoren bewegen:

- Anzahl der Erkenntnisse: Gibt an, wie oft diese Erkenntnis im ausgewählten Zeitraum generiert wurde.
- Schweregrad: Gibt den Schweregrad der Erkenntnis an, z. B. Mittel und Hoch.
- Prozentsatz: Gibt den Anteil dieses Erkenntnistyps im Kreisdiagramm an.
- Zuletzt generiert: Gibt an, wie viel Zeit seit der letzten Generierung dieses Erkenntnistyps vergangen ist.

Konten mit den meisten Erkenntnissen

Diese Einstellung bietet die folgenden Optionen:

- Konto: Gibt die AWS-Konto ID an, unter der das Ergebnis generiert wurde.
- Anzahl der Erkenntnisse: Gibt an, wie oft eine Erkenntnis für diese Konto-ID generiert wurde.
- Zuletzt generiert: Gibt an, wie viel Zeit seit der letzten Generierung dieses Erkenntnistyps vergangen ist.
- Hoher Schweregrad: Standardmäßig werden die Daten für die Erkenntnistypen mit hohem Schweregrad angezeigt. Mögliche Optionen für dieses Feld sind Hoher Schweregrad, Mittlerer Schweregrad und Gesamter Schweregrad.

Ressourcen mit Erkenntnissen

Diese Einstellung bietet die folgenden Optionen:

- Ressource: Gibt den potenziell betroffenen Ressourcentyp an. Wenn diese Ressource zu Ihrem Konto gehört, können Sie auf den Quicklink zugreifen, um die Ressourcendetails einzusehen. Wenn Sie ein GuardDuty Administratorkonto haben, können Sie die Details der potenziell betroffenen Ressource einsehen, indem Sie mit den Anmeldeinformationen des Mitgliedskontos, zu dem diese Ressource gehört, auf die GuardDuty Konsole zugreifen.
- Konto: Gibt die AWS-Konto ID an, zu der diese Ressource gehört.
- Anzahl der Erkenntnisse: Gibt an, wie oft diese Ressource mit einer Erkenntnis verknüpft wurde.
- Zuletzt generiert: Gibt an, wie viel Zeit seit der letzten Generierung dieses Erkenntnistyps vergangen ist.
- Alle Ressourcentypen: Standardmäßig werden die Daten für alle Ressourcentypen angezeigt. Mithilfe der Dropdownliste können Sie die Daten für einen bestimmten Ressourcentyp wie Instance AccessKey, Lambda und andere anzeigen.
- Hoher Schweregrad: Standardmäßig werden die Daten für die Erkenntnistypen mit hohem Schweregrad angezeigt. Mithilfe der Dropdownliste können Sie die Daten für andere Schweregrade anzeigen. Mögliche Optionen für dieses Feld sind Hoher Schweregrad, Mittlerer Schweregrad und Gesamter Schweregrad.

Am wenigsten auftretende Erkenntnisse

Dieser Abschnitt enthält Einzelheiten zu den Suchtypen, die in Ihrer AWS Umgebung nicht häufig generiert werden. Diese Einsichten können Ihnen helfen, ein neu auftretendes Bedrohungsmuster in Ihrer Umgebung zu untersuchen und entsprechende Maßnahmen zu ergreifen. Die Tabelle enthält die folgenden Daten:

- Erkenntnistyp: Gibt den Namen des Erkenntnistyps an.
- Anzahl der Erkenntnisse: Gibt an, wie oft diese Erkenntnis im ausgewählten Zeitraum generiert wurde.
- Zuletzt generiert: Gibt an, wie viel Zeit seit der letzten Generierung dieses Erkenntnistyps vergangen ist.
- Hoher Schweregrad: Standardmäßig werden die Daten für die Erkenntnistypen mit hohem Schweregrad angezeigt. Mögliche Optionen für dieses Feld sind Hoher Schweregrad, Mittlerer Schweregrad und Gesamter Schweregrad.

Geltungsbereich der Schutzpläne

In diesem Abschnitt finden Sie die Anzahl der aktiven Mitgliedskonten, die zu Ihrer Organisation gehören und für die in der aktuellen Konfiguration eine oder mehrere Funktionen und zusätzliche Funktionen (falls zutreffend) aktiviert wurden AWS-Region.

Nur ein delegierter GuardDuty Administrator kann die Statistiken für die Mitgliedskonten innerhalb seiner Organisation einsehen. Wenn eine Funktion nicht konfiguriert ist, wählen Sie in der Spalte Aktionen die Option Konfigurieren aus.

Wenn Sie eine neue AWS Organisation erstellen, kann es bis zu 24 Stunden dauern, bis die Statistiken für die gesamte Organisation generiert sind.

Feedback zum Zusammenfassungs-Dashboard geben

GuardDuty fordert Sie auf, Feedback zur Benutzerfreundlichkeit, den Funktionen und der Leistung des Übersichts-Dashboards zu geben. Dies wird uns helfen, das Dashboard zu verbessern.

Um Feedback zum Zusammenfassungs-Dashboard zu geben

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Zusammenfassung aus. Wenn Sie die GuardDuty Konsole öffnen, wird das Übersichts-Dashboard angezeigt.
3. Wählen Sie Feedback in der oberen rechten Ecke des Dashboards. Dadurch wird ein Formular geöffnet. Nachdem Sie das Feedback gegeben haben, wählen Sie Senden.

Filtern von Ergebnissen

Mit einem Erkenntnisfilter können Sie Erkenntnisse anzeigen, die den von Ihnen angegebenen Kriterien entsprechen, und alle nicht übereinstimmenden Erkenntnisse herausfiltern. Sie können Suchfilter ganz einfach mit der GuardDuty Amazon-Konsole oder mit der CreateFilterAPI mithilfe von JSON erstellen. Lesen Sie die folgenden Abschnitte, um zu erfahren, wie Sie einen Filter in der Konsole erstellen. Informationen zur Verwendung dieser Filter zur automatischen Archivierung eingehender Erkenntnisse finden Sie unter Unterdrückungsregeln.

Filter in der GuardDuty Konsole erstellen

Suchfilter können über die GuardDuty Konsole erstellt und getestet werden. Sie können über die Konsole erstellte Filter speichern, um sie in Unterdrückungsregeln oder zukünftigen Filtervorgängen

zu verwenden. Ein Filter besteht aus mindestens einem Filterkriterium, das aus einem Filterattribut in Kombination mit mindestens einem Wert besteht.

Beachten Sie beim Anlegen eines neuen Benutzers Folgendes:

- Filter akzeptieren keine Platzhalter.
- Sie können mindestens ein Attribut oder maximal 50 Attribute als Kriterien für einen bestimmten Filter angeben.
- Wenn Sie die Bedingung gleich zu oder ungleich zu verwenden, um nach einem Attributwert wie z. B. der Konto-ID zu filtern, können Sie maximal 50 Werte angeben.
- Jedes Filterkriterienattribut wird als `AND`-Operator ausgewertet. Mehrere Werte für dasselbe Attribut werden als `AND/OR` ausgewertet.

So filtern Sie Ergebnisse (Konsole)

1. Wählen Sie oberhalb der angezeigten Ergebnisliste die Option Filterkriterien hinzufügen GuardDuty aus.
2. Wählen Sie in der erweiterten Liste der Attribute die Attribute aus, die Sie als Kriterien für Ihren Filter angeben möchten, wie z. B. Konto-ID oder Aktionstyp.

   > **Note**
   >
   > Eine Liste der Attribute, die Sie als Filterkriterien angeben können, finden Sie in der Tabelle der Filterkriterien auf dieser Seite.

3. Geben Sie im angezeigten Textfeld für jedes ausgewählte Attribut einen Wert ein und wählen Sie dann Anwenden.

   > **Note**
   >
   > Nachdem Sie einen Filter angewendet haben, können Sie ihn so konvertieren, dass er Erkenntnisse ausschließt, die mit dem Filter übereinstimmen, indem Sie den schwarzen Punkt links neben dem Filternamen auswählen. Dadurch wird für das ausgewählte Attribut eigentlich der Filter "ungleich" erstellt.

4. Um die angegebenen Attribute und deren Werte (Filterkriterien) als Filter zu speichern, wählen Sie Save (Speichern). Geben Sie den Filternamen und die Filterbeschreibung ein und wählen Sie dann Fertig aus.

Filterattribute

Wenn Sie Filter erstellen oder Erkenntnisse mithilfe der API-Vorgänge sortieren, müssen Sie Filterkriterien in JSON angeben. Diese Filterkriterien korrelieren mit den JSON-Details einer Erkenntnis. Die folgende Tabelle enthält eine Liste der Konsolenanzeigenamen für Filterattribute und die entsprechenden JSON-Feldnamen.

Konsolen-Feldname	JSON-Feldname
Konto-ID	accountId
Die ID des Ergebnisses	id
Region	Region
Schweregrad	severity Wenn Sie `severity` mit API, AWS CLI, oder verwenden AWS CloudFormation, hat es einen numerischen Wert. Weitere Informationen finden Sie unter findingCriteria.
Ergebnistyp	Typ
Aktualisiert um	updatedAt
Access Key ID	Ressource. accessKeyDetails. accessKeyId
Haupt-ID	Ressource. accessKeyDetails. principalId
Username	Ressource. accessKeyDetails. userName
Benutzertyp	Ressource. accessKeyDetails. Benutzertyp
ID des IAM-Instance-Profils	Ressource.Instanzdetails. iamInstanceProfile.id

Konsolen-Feldname	JSON-Feldname
Instance-ID	resource.instanceDetails.instanceId
ID des Instance-Image	resource.instanceDetails.imageId
Instance-Tag-Schlüssel	resource.instanceDetails.tags.key
Instance-Tag-Wert	resource.instanceDetails.tags.value
IPv6-Adresse	resource.instanceDetails.networkInterfaces.ipv6Addresses
Private IPv4-Adresse	Ressource.Instanzdetails.Netzwerkschnittstellen. privateIpAddresses. privateIpAddress
Öffentlicher DNS-Name	Resource.InstanceDetails.Netzwerkschnittstellen. publicDnsName
Öffentliche IP	resource.instanceDetails.networkInterfaces.publicIp
Sicherheitsgruppen-ID	resource.instanceDetails.networkInterfaces.securityGroups.groupId
Name der Sicherheitsgruppe	resource.instanceDetails.networkInterfaces.securityGroups.groupName
Subnetz-ID	resource.instanceDetails.networkInterfaces.subnetId
VPC-ID	resource.instanceDetails.networkInterfaces.vpcId
Outpost-ARN	resource.instanceDetails.outpostARN
Ressourcentyp	resource.resourceType
Bucket-Berechtigungen	resource.s3 .publicAccess.EffectivePermission BucketDetails

Konsolen-Feldname	JSON-Feldname
Bucket-Name	resource.s3 BucketDetails .name
Bucket-Tag-Schlüssel	resource.s3 BucketDetails .tags.key
Bucket-Tag-Wert	resource.s3 BucketDetails .tags.value
Bucket-Typ	resource.s3 BucketDetails .type
Aktionstyp	service.action.actionType
Aufgerufene API	dienste.aktion. awsApiCallAktion.API
API-Aufrufertyp	Service.Aktion. awsApiCallAktion.Anrufertyp
API-Fehlercode	dienst.aktion. awsApiCallAktion.Fehlercode
Stadt des API-Aufrufers	Service.Aktion. awsApiCallAktion. remoteIpD etails.Stadt.Stadtname
Land des API-Aufrufers	dienst.aktion. awsApiCallAktion. remoteIpD etails. Land.Ländername
IPv4-Adresse des API-Aufrufers	dienst.aktion. awsApiCallAktion. remoteIpD etails.IP-Adresse v4
IPv6-Adresse des API-Aufrufers	service.action. awsApiCallAktion. remoteIpD etails.IP-Adresse V6
ASN-ID des API-Aufrufers	dienst.aktion. awsApiCallAktion. remoteIpD etails.organization.asn
ASN-Name des API-Aufrufers	dienste.aktion. awsApiCallAktion. remoteIpD etails. Organisation. ASNORG
Servicename des API-Aufrufers	Service.Aktion. awsApiCallAktion.Dienstname
DNS-Anforderungs-Domain	dienst.aktion. dnsRequestAction.domäne

Konsolen-Feldname	JSON-Feldname
Domainsuffix der DNS-Anforderung	service.action. dnsRequestAction. domainWith Suffix
Netzwerkverbindung blockiert	Service.Aktion. networkConnectionAction. blockiert
Netzwerkverbindungsrichtung	Service.Aktion. networkConnectionAction. Verbindungsrichtung
Netzwerkverbindung lokaler Port	dienst.aktion. networkConnectionAction. localPortDetails. Hafen
Netzwerkverbindungsprotokoll	Service.Aktion. networkConnectionAction. Protokoll
Netzwerkverbindung Stadt	Service.Aktion. networkConnectionAction. remoteIpDetails.Stadt.Stadtname
Netzwerkverbindung Land	dienst.aktion. networkConnectionAction. remoteIpDetails. Land.Landesname
Remote-IPv4-Adresse der Netzwerkverbindung	dienst.aktion. networkConnectionAction. remoteIpDetails. IP-Adresse v4
Netzwerkverbindung, Remote-IPv6-Adresse	service.action. networkConnectionAction. remoteIpDetails. IP-Adresse v6
Remote IP ASN-ID der Netzwerkverbindung	dienst.aktion. networkConnectionAction. remoteIpDetails.organisation.asn
Remote IP ASN-Name der Netzwerkverbindung	dienste.aktion. networkConnectionAction. remoteIpDetails. Organisation. ASNORG
Remote-Port der Netzwerkverbindung	Service.Aktion. networkConnectionAction. remotePortDetails. Hafen
Remote-Konto zugeordnet	Service.Aktion. awsApiCallAktion. remoteAcc ountDetails. angegliedert

Konsolen-Feldname	JSON-Feldname
IPv4-Adresse des Kubernetes-API-Aufrufers	Service. Aktion. kubernetesApiCallAktion. remoteIpDetails.IP-Adresse v4
IPv6-Adresse des Kubernetes-API-Aufrufers	service.action. kubernetesApiCallAktion. remoteIpDetails.IP-Adresse V6
Kubernetes-Namespace	dienst.aktion. kubernetesApiCallAktion.Namespace
ASN-ID des Kubernetes-API-Aufrufers	dienst.aktion. kubernetesApiCallAktion. remoteIpDetails.organization.asn
URI für die Kubernetes-API-Aufrufanforderung	dienste.aktion. kubernetesApiCallAktion.Anforderungs-URI
Kubernetes-API-Statuscode	dienst.aktion. kubernetesApiCallAktion.Statuscode
Lokale IPv4-Adresse der Netzwerkverbindung	dienste.aktion. networkConnectionAction. localIpDetails. IP-Adresse v4
Netzwerkverbindung, lokale IPv6-Adresse	service.action. networkConnectionAction. localIpDetails. IP-Adresse v6
Protokoll	dienst.aktion. networkConnectionAction. Protokoll
Servicename des API-Aufrufs	Service.Aktion. awsApiCallAktion.Dienstname
Konto-ID des API-Aufrufers	dienst.aktion. awsApiCallAktion. remoteAccountDetails. accountId
Name der Bedrohungsliste	Service. Zusätzliche Informationen. threatListName
Ressourcenrolle	service.resourceRole
EKS-Cluster-Name	Ressource. eksClusterDetails.name

Konsolen-Feldname	JSON-Feldname
Name des Kubernetes-Workloads	Resource.KubernetesEinzelheiten. kubernetesWorkloadDetails.name
Namespace des Kubernetes-Workloads	Resource.KubernetesEinzelheiten. kubernetesWorkloadDetails. Namespace
Kubernetes-Benutzername	Resource.KubernetesEinzelheiten. kubernetesUserDetails. Nutzername
Kubernetes-Container-Image	Resource.KubernetesEinzelheiten. kubernetesWorkloadDetails.containers.image
Kubernetes-Container-Image-Präfix	Resource.KubernetesEinzelheiten. kubernetesWorkloadDetails.containers.imagePräfix
Scan-ID	Dienst. ebsVolumeScanEinzelheiten. ScanID
Name der Bedrohung durch EBS Volume Scan	Dienst. ebsVolumeScanEinzelheiten. Scan-Erkennungen. threatDetectedByName.Bedrohungsnames.Name
Schweregrad der Bedrohung	Dienst. ebsVolumeScanEinzelheiten. Scan-Erkennungen. threatDetectedByName.Bedrohungsnames.Schweregrad
Datei-SHA	Dienst. ebsVolumeScanEinzelheiten. Scan-Erkennungen. threatDetectedByName.Bedrohungsnames.FilePaths.Hash
ECS-Cluster-Name	Ressource. ecsClusterDetails.name
ECS-Container-Image	Ressource. ecsClusterDetails.taskdetails.containers.image
ARN der ECS-Aufgabendefinition	Ressource. ecsClusterDetails.taskdetails.definitionARN
Eigenständiges Container-Image	resource.containerDetails.image

Konsolen-Feldname	JSON-Feldname
Datenbank-Instance-ID	Ressource. rdsDbInstanceEinzelheiten. dbInstanceIdentifier
Datenbank-Cluster-ID	Ressource. rdsDbInstanceEinzelheiten. dbClusterIdentifier
Datenbank-Engine	Ressource. rdsDbInstanceEinzelheiten. Motor
Datenbankbenutzer	Ressource. rdsDbUserEinzelheiten. Benutzer
Tag-Schlüssel der Datenbank-Instance	Ressource. rdsDbInstancedetails.tags.key
Tag-Wert der Datenbank-Instance	Ressource. rdsDbInstanceDetails.Tags.Wert
Ausführbare SHA-256	service.runtimeDetails.process.executableSha256
Prozessname	service.runtimeDetails.process.name
Pfad der ausführbaren Datei	service.runtimeDetails.process.executablePath
Lambda-Funktionsname	resource.lambdaDetails.functionName
ARN der Lambda-Funktion	resource.lambdaDetails.functionArn
Lambda-Funktions-Tag-Schlüssel	resource.lambdaDetails.tags.key
Tag-Wert der Lambda-Funktion	resource.lambdaDetails.tags.value
DNS-Anforderungs-Domain	Service.Aktion. dnsRequestAction. domainWithSuffix

Unterdrückungsregeln

Eine Unterdrückungsregel ist eine Reihe von Kriterien, die zum Filtern von Erkenntnissen verwendet werden, indem neue Erkenntnisse, die den angegebenen Kriterien entsprechen, automatisch archiviert werden. Unterdrückungsregeln können verwendet werden, um Ergebnisse mit niedrigem Wert, falsch positive Ergebnisse oder Bedrohungen zu filtern, auf die Sie nicht reagieren möchten,

sodass die Sicherheitsbedrohungen mit den meisten Auswirkungen auf Ihre Umgebung leichter zu erkennen sind.

Nachdem Sie eine Unterdrückungsregel erstellt haben, werden neue Ergebnisse, die den in der Regel definierten Kriterien entsprechen, automatisch archiviert, solange die Unterdrückungsregel gültig ist. Sie können einen vorhandenen Filter verwenden, um eine Unterdrückungsregel zu erstellen, oder einen neuen Filter für die Unterdrückungsregel definieren, während Sie sie erstellen. Sie können Unterdrückungsregeln so konfigurieren, dass ganze Ergebnistypen unterdrückt werden, oder detailliertere Filterkriterien definieren, damit nur bestimmte Instances eines bestimmten Ergebnistyps unterdrückt werden. Sie können die Unterdrückungsregeln jederzeit bearbeiten.

Unterdrückte Ergebnisse werden nicht an AWS Security Hub Amazon Simple Storage Service, Amazon Detective oder Amazon gesendet, wodurch der Geräuschpegel reduziert wird EventBridge, wenn Sie GuardDuty Ergebnisse über Security Hub, SIEM eines Drittanbieters oder andere Alarm- und Ticketing-Anwendungen nutzen. Wenn Sie diese Option aktiviert habenGuardDuty Schutz vor Schadsoftware, lösen die unterdrückten GuardDuty Ergebnisse keinen Malware-Scan aus.

GuardDuty generiert weiterhin Ergebnisse, auch wenn sie Ihren Unterdrückungsregeln entsprechen. Diese Ergebnisse werden jedoch automatisch als archiviert markiert. Das archivierte Ergebnis wird 90 Tage lang gespeichert und kann in GuardDuty diesem Zeitraum jederzeit eingesehen werden. Sie können unterdrückte Ergebnisse in der GuardDuty Konsole anzeigen, indem Sie in der Tabelle mit den Ergebnissen die Option Archiviert auswählen, oder Sie können die GuardDuty API über die ListFindingsAPI aufrufen, wobei das `findingCriteria` Kriterium `service.archived` wahr ist.

> **Note**
>
> In einer Umgebung mit mehreren Konten kann nur der GuardDuty Administrator Unterdrückungsregeln erstellen.

Häufige Anwendungsfälle für Unterdrückungsregeln und Beispiele

Die folgenden Erkenntnistypen werden häufig für die Anwendung von Unterdrückungsregeln verwendet. Wählen Sie den Namen der Erkenntnis aus, um mehr über diese Erkenntnis zu erfahren, oder überprüfen Sie die Informationen, um in der Konsole eine Unterdrückungsregel für diesen Erkenntnistyp zu erstellen.

> **Important**
>
> GuardDuty empfiehlt, dass Sie Unterdrückungsregeln reaktiv und nur für Ergebnisse erstellen, für die Sie wiederholt Fehlalarme identifiziert haben.

- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS – Verwenden Sie eine Unterdrückungsregel, die automatisch Erkenntnisse archiviert, die generiert werden, falls das VPC-Netzwerk so konfiguriert ist, dass der Internet-Datenverkehr über ein On-Premises-Gateway anstelle eines VPC-Internet-Gateways weitergeleitet wird.

  Diese Erkenntnis wird generiert, wenn das Netzwerk so konfiguriert ist, dass der Internetverkehr von einem On-Premises-Gateway und nicht von einem VPC Internet Gateway (IGW) ausgeht. Geläufige Konfigurationen, z. B. die Verwendung von AWS Outposts, oder VPC-VPN-Verbindungen, können dazu führen, dass Datenverkehr auf diese Weise weitergeleitet wird. Wenn dies ein erwartetes Verhalten ist, empfiehlt es sich, Unterdrückungsregeln in zu verwenden und eine Regel zu erstellen, die aus zwei Filterkriterien besteht. Das erste Kriterium ist der Ergebnistyp, der `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS` sein sollte. Das zweite Filterkriterium ist die IPv4-Adresse des API-Aufrufers mit der IP-Adresse oder dem CIDR-Bereich Ihres On-Premises-Internet-Gateways. Das folgende Beispiel stellt den Filter dar, den Sie verwenden würden, um diesen Erkenntnistyp auf der Grundlage der IP-Adresse des API-Aufrufers zu unterdrücken.

  ```
  Finding type: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
   API caller IPv4 address: 198.51.100.6
  ```

  > **Note**
  >
  > Um mehrere API-Aufrufer-IPs einzubeziehen, können Sie für jede IPv4-Adressfilter für API-Anrufer einen neuen API-Anrufer-IPv4-Adressfilter hinzufügen.

- Recon:EC2/Portscan – Verwenden Sie eine Unterdrückungsregel, um Erkenntnisse automatisch zu aktivieren, wenn Sie eine Anwendung für Schwachstellenanalysen verwenden.

  Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `Recon:EC2/Portscan` verwenden. Das zweite Filterkriterium sollte den Instances entsprechen, die diese Tools zur Schwachstellenanalyse hosten. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon,

welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Das folgende Beispiel stellt den Filter dar, den Sie verwenden würden, um diesen Erkenntnistyp auf der Grundlage von Instances mit einem bestimmten AMI zu unterdrücken.

```
Finding type: Recon:EC2/Portscan Instance image ID: ami-999999999
```

- UnauthorizedAccess:EC2/SSHBruteForce – Verwenden Sie eine Unterdrückungsregel, um Erkenntnisse, die sich auf Bastion-Instances beziehen, automatisch zu archivieren.

  Wenn das Ziel des Brute-Force-Versuchs ein Bastion-Host ist, kann dies ein erwartetes Verhalten für Ihre Umgebung sein. AWS In diesem Fall sollten Sie für dieses Ergebnis eine Unterdrückungsregel einrichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `UnauthorizedAccess:EC2/SSHBruteForce` verwenden. Das zweite Filterkriterium sollte den Instances entsprechen, die als Bastion-Host eingesetzt werden. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Das folgende Beispiel stellt den Filter dar, den Sie verwenden würden, um diesen Erkenntnistyp auf der Grundlage von Instances mit einem bestimmten Instance-Tag-Wert zu unterdrücken.

  ```
  Finding type: UnauthorizedAccess:EC2/SSHBruteForce Instance tag value: devops
  ```

- Recon:EC2/PortProbeUnprotectedPort – Verwenden Sie eine Unterdrückungsregel, um Erkenntnisse automatisch zu archivieren, wenn sie auf absichtlich exponierte Instances ausgerichtet ist.

  In einigen Fällen werden Instances absichtlich exponiert, weil sie beispielsweise Web-Server hosten. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für dieses Ergebnis einzurichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `Recon:EC2/PortProbeUnprotectedPort` verwenden. Das zweite Filterkriterium sollte den Instances entsprechen, die als Bastion-Host eingesetzt werden. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Das folgende Beispiel stellt den Filter dar, den Sie verwenden würden, um diesen Erkenntnistyp auf der Grundlage von Instances mit einem bestimmten Instance-Tag-Schlüssel in der Konsole zu unterdrücken.

  ```
  Finding type: Recon:EC2/PortProbeUnprotectedPort Instance tag key: prod
  ```

Empfohlene Unterdrückungsregeln für Ergebnisse von Runtime Monitoring

- PrivilegeEscalation:Runtime/DockerSocketAccessed wird generiert, wenn ein Prozess in einem Container mit dem Docker-Socket kommuniziert. Möglicherweise gibt es Container in Ihrer Umgebung, die aus legitimen Gründen auf den Docker-Socket zugreifen müssen. Der Zugriff von solchen Containern generiert PrivilegeEscalation:Runtime/DockerSocketAccessed-Erkenntnisse. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für diesen Befundtyp einzurichten. Das erste Kriterium sollte das Attribut Erkenntnistyp mit dem Wert `PrivilegeEscalation:Runtime/DockerSocketAccessed` verwenden. Das zweite Filterkriterium ist das Feld Ausführbarer Pfad mit einem Wert, der dem Wert des Prozesses `executablePath` in der generierten Erkenntnis entspricht. Alternativ kann das zweite Filterkriterium das Feld Ausführbare SHA-256 verwenden, dessen Wert dem `executableSha256` des Prozesses in der generierten Erkenntnis entspricht.
- Kubernetes-Cluster führen ihre eigenen DNS-Server als Pods aus, z. B. `coredns`. Daher werden bei jeder DNS-Suche in einem Pod zwei DNS-Ereignisse GuardDuty erfasst — eines vom Pod und das andere vom Server-Pod. Dadurch können Duplikate für die folgenden DNS-Erkenntnisse generiert werden:
  - Backdoor:Runtime/C&CActivity.B!DNS
  - CryptoCurrency:Runtime/BitcoinTool.B!DNS
  - Impact:Runtime/AbusedDomainRequest.Reputation
  - Impact:Runtime/BitcoinDomainRequest.Reputation
  - Impact:Runtime/MaliciousDomainRequest.Reputation
  - Impact:Runtime/SuspiciousDomainRequest.Reputation
  - Trojan:Runtime/BlackholeTraffic!DNS
  - Trojan:Runtime/DGADomainRequest.C!DNS
  - Trojan:Runtime/DriveBySourceTraffic!DNS
  - Trojan:Runtime/DropPoint!DNS
  - Trojan:Runtime/PhishingDomainRequest!DNS

  Die doppelten Erkenntnisse umfassen Pod-, Container- und Prozessdetails, die Ihrem DNS-Server-Pod entsprechen. Sie können mithilfe dieser Felder eine Unterdrückungsregel einrichten, um diese doppelten Erkenntnisse zu unterdrücken. Die ersten Filterkriterien sollten das Feld Erkenntnistyp verwenden, dessen Wert einem DNS-Erkenntnistyp aus der Liste der Erkenntnisse entspricht, die weiter oben in diesem Abschnitt bereitgestellt wurde. Das zweite Filterkriterium könnte entweder ausführbarer Pfad mit einem Wert sein, der dem Wert Ihres DNS-Servers

entspricht, `executablePath` oder Ausführbare SHA-256 mit einem Wert, der dem Wert Ihres DNS-Servers `executableSHA256` in der generierten Erkenntnis entspricht. Als optionales drittes Filterkriterium können Sie das Feld Kubernetes-Container-Image verwenden, dessen Wert dem Container-Image Ihres DNS-Server-Pods in der generierten Erkenntnis entspricht.

Regeln zur Unterdrückung erstellen

Wählen Sie Ihre bevorzugte Zugriffsmethode, um eine Unterdrückungsregel für die GuardDuty Suche nach Typen zu erstellen.

Console

Sie können Unterdrückungsregeln mithilfe der GuardDuty Konsole visualisieren, erstellen und verwalten. Unterdrückungsregeln werden auf die gleiche Weise wie Filter generiert, und Ihre vorhandenen gespeicherten Filter können als Unterdrückungsregeln verwendet werden. Weitere Informationen zum Erstellen von Filtern finden Sie unter Filtern von Ergebnissen.

So erstellen Sie eine Unterdrückungsregel mithilfe der Konsole:

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie auf der Seite Erkenntnisse die Option „Erkenntnisse unterdrücken“, um das Fenster mit den Unterdrückungsregeln zu öffnen.
3. Um das Menü mit den Filterkriterien zu öffnen, geben Sie **`filter criteria`** in Filterkriterien hinzufügen ein. Sie können ein Kriterium aus der Liste auswählen. Geben Sie einen gültigen Wert für das gewählte Kriterium ein.

> **Note**
>
> Um den gültigen Wert zu ermitteln, sehen Sie sich die Erkenntnistabelle an und wählen Sie eine Erkenntnis aus, die Sie unterdrücken möchten. Überprüfen Sie die Details im Erkenntnisfenster.

Sie können mehrere Filterkriterien hinzufügen und sicherstellen, dass nur die Erkenntnisse in der Tabelle erscheinen, die Sie unterdrücken möchten.

4. Geben Sie einen Namen und eine Beschreibung für die Unterdrückungsregel ein. Gültige Zeichen sind alphanumerische Zeichen, Punkt (.), Bindestrich (-), Unterstrich (_) und Leerzeichen.
5. Wählen Sie Speichern.

Sie können auch eine Unterdrückungsregel aus einem vorhandenen gespeicherten Filter erstellen. Weitere Informationen zum Erstellen von Filtern finden Sie unter Filtern von Ergebnissen.

So erstellen Sie eine Unterdrückungsregel aus einem gespeicherten Filter:

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie auf der Seite Erkenntnisse die Option Erkenntnisse unterdrücken, um das Fenster mit den Unterdrückungsregeln zu öffnen.
3. Wählen Sie in der Dropdownliste Gespeicherte Regeln einen gespeicherten Filter aus.
4. Sie können auch neue Filterkriterien hinzufügen. Wenn Sie keine zusätzlichen Filterkriterien benötigen, überspringen Sie diesen Schritt.

   Um das Menü mit den Filterkriterien zu öffnen, geben Sie **`filter criteria`** in Filterkriterien hinzufügen ein. Sie können ein Kriterium aus der Liste auswählen. Geben Sie einen gültigen Wert für das gewählte Kriterium ein.

   > **Note**
   >
   > Um den gültigen Wert zu ermitteln, sehen Sie sich die Erkenntnistabelle an und wählen Sie eine Erkenntnis aus, die Sie unterdrücken möchten. Überprüfen Sie die Details im Erkenntnisfenster.

5. Geben Sie einen Namen und eine Beschreibung für die Unterdrückungsregel ein. Gültige Zeichen sind alphanumerische Zeichen, Punkt (.), Bindestrich (-), Unterstrich (_) und Leerzeichen.
6. Wählen Sie Speichern.

API/CLI

So erstellen Sie eine Unterdrückungsregel mithilfe der API:

1. Sie können Unterdrückungsregeln auch über die CreateFilter-API erstellen. Geben Sie dazu die Filterkriterien in einer JSON-Datei an und folgen Sie dabei dem Format des unten beschriebenen Beispiels. Im folgenden Beispiel werden alle nicht archivierten Erkenntnisse mit niedrigem Schweregrad unterdrückt, die eine DNS-Anfrage an die Domain test.example.com enthalten. Bei Erkenntnissen mit mittlerem Schweregrad ist die Eingabeliste `["4", "5", "7"]`. Bei Erkenntnissen mit hohem Schweregrad ist die Eingabeliste `["6", "7", "8"]`. Sie können auch auf der Grundlage eines beliebigen Werts in der Liste filtern.

```
{
    "Criterion": {
        "service.archived": {
            "Eq": [
                "false"
            ]
        },
        "service.action.dnsRequestAction.domain": {
            "Eq": [
                "test.example.com"
            ]
        },
        "severity": {
            "Eq": [
                "1",
                "2",
                "3"
            ]
        }
    }
}
```

   Eine Liste der JSON-Feldnamen und deren Konsolenäquivalent finden Sie unter Filterattribute.

   Verwenden Sie zum Testen Ihrer Filterkriterien dasselbe JSON-Kriterium in der ListFindings-API und vergewissern Sie sich, dass die richtigen Erkenntnisse ausgewählt wurden. Um

Ihre Filterkriterien zu testen, AWS CLI folgen Sie dem Beispiel mit Ihrer eigenen detectorId- und .json-Datei.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty list-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
finding-criteria file://criteria.json
```

2. Laden Sie Ihren Filter, der als Unterdrückungsregel verwendet werden soll, mit der CreateFilter-API oder über die AWS -CLI hoch, indem Sie dem unten stehenden Beispiel folgen und Ihre eigene Detektor-ID, einen Namen für die Unterdrückungsregel und eine JSON-Datei angeben.

   Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty create-filter --action ARCHIVE --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name yourfiltername --finding-criteria
 file://criteria.json
```

Mit der ListFilter-API können Sie sich programmgesteuert eine Liste Ihrer Filter anzeigen lassen. Sie können die Details eines einzelnen Filters anzeigen, indem Sie der GetFilter-API den Filternamen zur Verfügung stellen. Aktualisieren Sie Filter mithilfe von UpdateFilter oder löschen Sie sie mit der DeleteFilter-API.

Löschen von Unterdrückungsregeln

Wählen Sie Ihre bevorzugte Zugriffsmethode, um eine Unterdrückungsregel für die GuardDuty Suche nach Typen zu löschen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

2. Wählen Sie auf der Seite Erkenntnisse die Option Erkenntnisse unterdrücken, um das Fenster mit den Unterdrückungsregeln zu öffnen.
3. Wählen Sie in der Dropdownliste Gespeicherte Regeln einen gespeicherten Filter aus.
4. Klicken Sie auf Delete rule (Regel löschen).

API/CLI

Führen Sie die API DeleteFilter aus. Geben Sie den Filternamen und die zugehörige Melder-ID für die jeweilige Region an.

Alternativ können Sie das folgende AWS CLI Beispiel verwenden, indem Sie die *rot* formatierten Werte ersetzen:

```
aws guardduty delete-filter --region us-east-1 --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --filter-name filterName
```

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

Arbeiten mit vertrauenswürdigen IP- und Bedrohungslisten

Amazon GuardDuty überwacht die Sicherheit Ihrer AWS Umgebung, indem es VPC-Flow-Logs, AWS CloudTrail Event-Logs und DNS-Logs analysiert und verarbeitet. Sie können diesen Überwachungsumfang anpassen, indem Sie ihn so konfigurieren GuardDuty , dass Benachrichtigungen für vertrauenswürdige IP-Adressen aus Ihren eigenen Listen für vertrauenswürdige IP-Adressen und Warnungen vor bekannten bösartigen IP-Adressen aus Ihren eigenen Bedrohungslisten gestoppt werden.

Vertrauenswürdige IP-Adressen-Listen und Bedrohungslisten gelten nur für Datenverkehr, der an öffentlich routingfähige IP-Adressen geleitet wird. Die Auswirkungen einer Liste gelten für alle VPC-Flow-Protokolle und CloudTrail -Ergebnisse, gelten jedoch nicht für DNS-Ergebnisse.

GuardDuty kann für die Verwendung der folgenden Listentypen konfiguriert werden.

Liste vertrauenswürdiger IPs

Listen vertrauenswürdiger IP-Adressen bestehen aus IP-Adressen, denen Sie für die sichere Kommunikation mit Ihrer AWS Infrastruktur und Ihren Anwendungen vertraut haben.

GuardDuty generiert kein VPC-Flow-Protokoll oder CloudTrail Ergebnisse für IP-Adressen auf vertrauenswürdigen IP-Listen. Sie können maximal 2000 IP-Adressen und CIDR-Bereiche in einer einzigen Liste zuverlässiger IPs aufnehmen. Es kann immer nur eine Liste vertrauenswürdiger IPs pro AWS -Konto pro Region hochgeladen werden.

Liste der bedrohlichen IP-Adressen

Bedrohungslisten enthalten bekannte schädliche IP-Adressen. Diese Liste kann von Bedrohungsdaten von Drittanbietern stammen oder speziell für Ihr Unternehmen erstellt werden. Generiert nicht nur Ergebnisse aufgrund einer potenziell verdächtigen Aktivität, GuardDuty sondern generiert auch Ergebnisse auf der Grundlage dieser Bedrohungslisten. Sie können maximal 250.000 IP-Adressen und CIDR-Bereiche in eine einzige Bedrohungsliste aufnehmen. GuardDuty generiert nur Ergebnisse auf der Grundlage einer Aktivität, die IP-Adressen und CIDR-Bereiche in Ihren Bedrohungslisten umfasst. Die Ergebnisse werden nicht auf der Grundlage der Domainnamen generiert. Zu jedem Zeitpunkt können Sie AWS-Konto pro Region bis zu sechs hochgeladene Bedrohungslisten haben.

> **Note**
>
> Wenn Sie dieselbe IP-Adresse sowohl in eine Liste vertrauenswürdiger IP-Adressen als auch in eine Bedrohungsliste aufnehmen, wird sie zuerst von der Liste vertrauenswürdiger IP-Adressen verarbeitet und es wird keine Erkenntnis generiert.

In Umgebungen mit mehreren Konten können nur Benutzer mit GuardDuty Administratorkonten vertrauenswürdige IP-Adressen und Bedrohungslisten hinzufügen und verwalten. Listen vertrauenswürdiger IP-Adressen und Bedrohungslisten, die vom Administratorkonto hochgeladen werden, wirken sich negativ auf die GuardDuty Funktionalität der Mitgliedskonten aus. Mit anderen Worten: Bei Mitgliedskonten werden Ergebnisse auf der Grundlage von Aktivitäten GuardDuty generiert, bei denen es sich um bekannte bösartige IP-Adressen aus den Bedrohungslisten des Administratorkontos handelt, und es werden keine Ergebnisse generiert, die auf Aktivitäten basieren, die IP-Adressen aus den vertrauenswürdigen IP-Listen des Administratorkontos betreffen. Weitere Informationen finden Sie unter Verwaltung mehrerer Konten bei Amazon GuardDuty.

Listenformate

GuardDuty akzeptiert Listen in den folgenden Formaten.

Die maximale Größe der Datei, die die Liste zuverlässiger IPs oder die Bedrohungsliste hostet, ist 35 MB. In den Listen der vertrauenswürdigen IPs und der bedrohlichen IPs müssen die IP-Adressen und CIDR-Bereiche einzeln pro Zeile erscheinen. Es werden ausschließlich IPv4-Adressen akzeptiert.

- Klartext (TXT)

  Dieses Format unterstützt sowohl CIDR-Block- als auch individuelle IP-Adressen. Die folgende Beispielliste verwendet das Klartext-Format (TXT).

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

- Structured Threat Information Expression (STIX)

  Dieses Format unterstützt sowohl CIDR-Block- als auch individuelle IP-Adressen. Die folgende Beispielliste verwendet das STIX-Format.

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:ttp="http://stix.mitre.org/TTP-1"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
    http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.2/
stix_core.xsd
    http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.2/
campaign.xsd
    http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.2/
indicator.xsd
    http://stix.mitre.org/TTP-2 http://stix.mitre.org/XMLSchema/ttp/1.2/ttp.xsd
    http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/
default_vocabularies/1.2.0/stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 http://cybox.mitre.org/XMLSchema/
objects/Address/2.1/Address_Object.xsd"
    id="example:STIXPackage-a78fc4e3-df94-42dd-a074-6de62babfe16"
```

```
    version="1.2">
    <stix:Observables cybox_major_version="1" cybox_minor_version="1">
        <cybox:Observable id="example:observable-80b26f43-
dc41-43ff-861d-19aff31e0236">
            <cybox:Object id="example:object-161a5438-1c26-4275-ba44-a35ba963c245">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">

 <AddressObject:Address_Valuecondition="InclusiveBetween">192.0.2.0##comma##192.0.2.255</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable id="example:observable-b442b399-aea4-436f-bb34-
b9ef6c5ed8ab">
            <cybox:Object id="example:object-b422417f-bf78-4b34-ba2d-de4b09590a6d">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>198.51.100.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable
 id="example:observable-1742fa06-8b5e-4449-9d89-6f9f32595784">
            <cybox:Object id="example:object-dc73b749-8a31-46be-803f-71df77565391">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>203.0.113.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
    </stix:Observables>
</stix:STIX_Package>
```

- Open Threat Exchange (OTX)™ CSV

  Dieses Format unterstützt sowohl CIDR-Block- als auch individuelle IP-Adressen. Die folgende Beispielliste verwendet das OTX™-CSV-Format.

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
```

```
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

- FireEye™ iSight Threat Intelligence CSV

  Dieses Format unterstützt sowohl CIDR-Block- als auch individuelle IP-Adressen. Die folgende Beispielliste verwendet ein `FireEye`™-CSV-Format.

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp,
 subject, recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier,
 md5, sha1, sha256, description, fileType, packer, userAgent, registry,
 fileCompilationDateTime, filePath, asn, cidr, domain, domainTimeOfLookup,
 networkIdentifier, ip, port, protocol, registrantEmail, registrantName, networkType,
 url, malwareFamily, malwareFamilyId, actor, actorId, observationTime

01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,
 Related, , , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400

01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 198.51.100.1, , , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400
```

- Proofpoint™ ET Intelligence Feed CSV

  Dieses Format unterstützt ausschließlich individuelle IP-Adressen. Die folgende Beispielliste verwendet das `Proofpoint`-CSV-Format. Der Parameter `ports` ist optional. Wenn Sie den Port überspringen, achten Sie darauf, am Ende ein Komma (,) zu hinterlassen.

```
ip, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
```

```
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

- AlienVault™ Reputationsfeed

  Dieses Format unterstützt ausschließlich individuelle IP-Adressen. Die folgende Beispielliste verwendet das `AlienVault`-Format.

```
198.51.100.1#4#2#Malicious Host#US##0.0,0.0#3
203.0.113.1#4#2#Malicious Host#US##0.0,0.0#3
```

Erforderliche Berechtigungen für das Hochladen von Listen mit vertrauenswürdigen IPs und Bedrohungslisten

Verschiedene IAM-Identitäten erfordern spezielle Berechtigungen, um mit vertrauenswürdigen IP-Listen und Bedrohungslisten in arbeiten zu können. GuardDuty Eine Identität, der die verwaltete Richtlinie AmazonGuardDutyFullAccess angefügt ist, kann nur hochgeladene Listen mit vertrauenswürdigen IPs und Bedrohungslisten umbenennen und deaktivieren.

Um verschiedenen Identitäten vollen Zugriff auf die Arbeit mit vertrauenswürdigen IP-Listen und Bedrohungslisten zu erteilen (dies umfasst neben dem Umbenennen und Deaktivieren auch das Hinzufügen, Aktivieren, Löschen und Aktualisieren des Speicherorts oder der Namen der Listen), stellen Sie sicher, dass die folgenden Aktionen in der einem Benutzer, einer Gruppe oder einer Rolle zugewiesenen Berechtigungsrichtlinie vorhanden sind:

```
{
    "Effect": "Allow",
    "Action": [
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::555555555555:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

> **Important**
>
> Diese Aktionen sind nicht in der verwalteten Richtlinie `AmazonGuardDutyFullAccess` enthalten.

Verwenden der serverseitigen Verschlüsselung für Listen vertrauenswürdiger IPs und Bedrohungslisten

GuardDuty unterstützt die folgenden Verschlüsselungstypen für Listen: SSE-AES256 und SSE-KMS. SSE-C wird nicht unterstützt. Weitere Informationen zu Verschlüsselungstypen für S3 finden Sie unter Schützen von Daten mit serverseitiger Verschlüsselung.

Wenn Ihre Liste mit serverseitiger Verschlüsselung SSE-KMS verschlüsselt ist, müssen Sie der GuardDuty dienstbezogenen Rolle die AWSServiceRoleForAmazonGuardDutyBerechtigung zum Entschlüsseln der Datei erteilen, um die Liste zu aktivieren. Fügen Sie der KMS-Schlüsselrichtlinie die folgende Anweisung hinzu und ersetzen Sie die Konto-ID durch Ihre eigene:

```
{
    "Sid": "AllowGuardDutyServiceRole",
    "Effect": "Allow",
    "Principal": {
    "AWS": "arn:aws:iam::123456789123:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty"
    },
    "Action": "kms:Decrypt*",
    "Resource": "*"
}
```

Hinzufügen und Aktivieren einer vertrauenswürdigen IP-Liste oder einer Bedrohungs-IP-Liste

Wählen Sie eine der folgenden Zugriffsmethoden, um eine vertrauenswürdige IP-Liste oder eine Bedrohungs-IP-Liste hinzuzufügen und zu aktivieren.

Console

(Optional) Schritt 1: Den Standort-URL Ihrer Liste abrufen

1. Öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie im Navigationsbereich die Option Buckets aus.
3. Wählen Sie den Amazon-S3-Bucket-Namen, der die spezifische Liste enthält, die Sie hinzufügen möchten.
4. Wählen Sie den Namen des Objekts (Liste), um dessen Details anzuzeigen.
5. Kopieren Sie auf der Registerkarte Eigenschaften den S3-URI für dieses Objekt.

Schritt 2: Hinzufügen einer Liste vertrauenswürdiger IP-Adressen oder einer Bedrohungsliste

> **Important**
>
> Es kann immer nur eine Liste vertrauenswürdiger IPs hochgeladen werden. In ähnlicher Weise können Sie bis zu sechs Bedrohungslisten haben.

1. Öffnen Sie die Konsole unter https://console.aws.amazon.com/guardduty/. GuardDuty
2. Wählen Sie im Navigationsbereich Listen.
3. Klicken Sie auf der Seite List management auf Add a trusted IP list oder Add a threat list.
4. Je nach Ihrer Auswahl wird ein Dialogfeld angezeigt. Gehen Sie wie folgt vor:
   a. In Name der Liste geben Sie einen Namen für Ihre Liste ein.

      Einschränkungen bei der Benennung von Listen — Der Name Ihrer Liste kann Kleinbuchstaben, Großbuchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.
   b. Geben Sie unter Standort den Ort an, an dem Sie Ihre Liste hochgeladen haben. Falls Sie den Standort noch nicht haben, finden Sie weitere Informationen unter Step 1: Fetching location URL of your list.

      Format der Standort-URL

      - https://s3.amazonaws.com/bucket.name/file.txt
      - https://s3-aws-region.amazonaws.com/bucket.name/file.txt
      - http://bucket.s3.amazonaws.com/file.txt
      - http://bucket.s3-aws-region.amazonaws.com/file.txt
      - s3://bucket.name/file.txt
   c. Aktivieren Sie das Kontrollkästchen I agree.
   d. Wählen Sie Liste hinzufügen. Standardmäßig ist der Status der hinzugefügten Liste Inaktiv. Damit die Liste gültig ist, müssen Sie sie aktivieren.

Schritt 3: Hinzufügen einer Liste vertrauenswürdiger IP-Adressen oder einer Bedrohungsliste

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

2. Wählen Sie im Navigationsbereich Listen.
3. Wählen Sie auf der Seite Listenverwaltung die Liste aus, die Sie aktivieren möchten.
4. Wählen Sie Aktionen und dann Aktivieren. Die Aktivierung der Liste dauert bis zu 15 Minuten.

API/CLI

Für Listen vertrauenswürdiger IPs

- Führen Sie CreateIPSet aus. Stellen Sie sicher, dass Sie die `detectorId` des Mitgliedskontos angeben, für das Sie diese Liste vertrauenswürdiger IP-Adressen erstellen möchten.

  Einschränkungen bei der Benennung von Listen — Der Name Ihrer Liste kann Kleinbuchstaben, Großbuchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.

  - Sie können dies auch tun, indem Sie den folgenden AWS Command Line Interface - Befehl ausführen und sicherstellen, dass Sie die `detector-id` durch die Detektor-ID des Mitgliedskontos ersetzen, für das Sie die Liste der vertrauenswürdigen IP-Adressen aktualisieren möchten.

    ```
    aws guardduty create-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
     --name AnyOrganization List --format Plaintext --location https://
    s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/DOC-EXAMPLE-SOURCE-FILE.format --
    activate
    ```

Für Bedrohungslisten

- Führen Sie CreateThreatIntelSet. Stellen Sie sicher, dass Sie die `detectorId` des Mitgliedskontos angeben, für das Sie diese Bedrohungsliste erstellen möchten.
  - Sie können dies auch tun, indem Sie den folgenden Befehl ausführen. AWS Command Line Interface Stellen Sie sicher, dass Sie die `detectorId` des Mitgliedskontos angeben, für das Sie eine Bedrohungsliste erstellen möchten.

    ```
    aws guardduty create-threat-intel-set --detector-
    id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --
    format Plaintext --location https://s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/
    DOC-EXAMPLE-SOURCE-FILE.format --activate
    ```

> **Note**
>
> Nachdem Sie eine IP-Liste aktiviert oder aktualisiert haben, GuardDuty kann es bis zu 15 Minuten dauern, bis die Liste synchronisiert ist.

Aktualisieren von Listen zuverlässiger IPs und Bedrohungslisten

Sie können den Namen einer Liste oder die IP-Adressen aktualisieren, die einer Liste hinzugefügt wurden, die bereits hinzugefügt und aktiviert wurde. Wenn Sie eine Liste aktualisieren, müssen Sie sie erneut aktivieren, GuardDuty um die neueste Version der Liste verwenden zu können.

Wählen Sie eine der Zugriffsmethoden, um eine vertrauenswürdige IP oder Bedrohungsliste zu aktualisieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Listen.
3. Wählen Sie auf der Seite Listenverwaltung den Satz vertrauenswürdiger IP-Adressen oder eine Bedrohungsliste aus, die Sie aktualisieren möchten.
4. Wählen Sie Aktionen und anschließend Bearbeiten.
5. Aktualisieren Sie die Informationen im Dialogfeld Liste aktualisieren nach Bedarf.

   Einschränkungen bei der Benennung von Listen — Der Name Ihrer Liste kann Kleinbuchstaben, Großbuchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.
6. Aktivieren Sie das Kontrollkästchen Ich stimme zu und wählen Sie dann Liste aktualisieren. Der Wert in der Spalte Status ändert sich auf Inaktiv.
7. Reaktivierung der aktualisierten Liste

   a. Wählen Sie auf der Seite Listenverwaltung die Liste aus, die Sie aktivieren möchten.

   b. Wählen Sie Aktionen und dann Aktivieren.

API/CLI

1. Führen Sie UpdateIPSet aus, um eine Liste vertrauenswürdiger IP-Adressen zu aktualisieren.

- Sie können dies auch tun, indem Sie den folgenden AWS CLI -Befehl ausführen und sicherstellen, dass Sie die `detector-id` durch die Detektor-ID des Mitgliedskontos ersetzen, für das Sie die Liste der vertrauenswürdigen IP-Adressen aktualisieren möchten.

```
aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
activate
```

2. Führen Sie UpdateThreatIntelSet aus, um eine Bedrohungsliste zu aktualisieren
   - Sie können dies auch tun, indem Sie den folgenden AWS CLI -Befehl ausführen und sicherstellen, dass Sie die `detector-id` durch die Detektor-ID des Mitgliedskontos ersetzen, für das Sie die Bedrohungsliste aktualisieren möchten.

```
aws guardduty update-threatintel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
intel-set-id d4b94fc952d6912b8f3060768example --activate
```

Deaktivieren oder Löschen einer vertrauenswürdigen IP- oder Bedrohungsliste

Wählen Sie eine der Zugriffsmethoden, um eine Liste vertrauenswürdiger IPs oder eine Bedrohungsliste zu löschen (mithilfe der Konsole) oder zu deaktivieren (mithilfe der API/CLI).

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Listen.
3. Wählen Sie auf der Seite Listenverwaltung die Liste aus, die Sie löschen möchten.
4. Wählen Sie Aktionen und anschließend Löschen.
5. Bestätigen Sie die Aktion und wählen Sie Löschen. Die spezifische Liste ist in der Tabelle nicht mehr verfügbar.

API/CLI

1. Für eine Liste vertrauenswürdiger IPs

   Führen Sie UpdateIPSet aus, um eine Liste vertrauenswürdiger IP-Adressen zu aktualisieren.

   - Sie können dies auch tun, indem Sie den folgenden AWS CLI -Befehl ausführen und sicherstellen, dass Sie die `detector-id` durch die Detektor-ID des Mitgliedskontos ersetzen, für das Sie die Liste der vertrauenswürdigen IP-Adressen aktualisieren möchten.

     Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/ -Konsole.

     ```
     aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
      --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
     no-activate
     ```

2. Für eine Bedrohungsliste

   Führen Sie UpdateThreatIntelSet aus, um eine Bedrohungsliste zu aktualisieren

   - Alternativ können Sie den folgenden AWS CLI -Befehl ausführen, um eine Liste vertrauenswürdiger IPs zu aktualisieren. Achten Sie dabei darauf, die `detector-id` durch die Detektor-ID des Mitgliedskontos zu ersetzen, für das Sie die Bedrohungsliste aktualisieren möchten.

     ```
     aws guardduty update-threatintel-set --detector-
     id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
     intel-set-id d4b94fc952d6912b8f3060768example --no-activate
     ```

Exportieren von Erkenntnissen

GuardDuty bewahrt die generierten Ergebnisse für einen Zeitraum von 90 Tagen auf. GuardDuty exportiert die aktiven Ergebnisse nach Amazon EventBridge (EventBridge). Sie können die generierten Ergebnisse optional in einen Amazon Simple Storage Service (Amazon S3) -Bucket exportieren. Auf diese Weise können Sie die historischen Daten potenziell verdächtiger Aktivitäten in Ihrem Konto nachverfolgen und beurteilen, ob die empfohlenen Abhilfemaßnahmen erfolgreich waren.

Alle neuen aktiven Ergebnisse, die GuardDuty generiert werden, werden innerhalb von etwa 5 Minuten nach der Generierung des Ergebnisses automatisch exportiert. Sie können die Häufigkeit festlegen, in die Aktualisierungen der aktiven Ergebnisse exportiert werden EventBridge. Die Häufigkeit, die Sie auswählen, gilt für den Export neuer Vorkommen vorhandener Ergebnisse in Ihren S3-Bucket (sofern konfiguriert) und Detective (falls integriert). EventBridge Informationen darüber, wie mehrere Vorkommen vorhandener Ergebnisse GuardDuty aggregiert werden, finden Sie unter. GuardDuty Aggregation finden

Wenn Sie Einstellungen für den Export von Ergebnissen in einen Amazon S3 S3-Bucket konfigurieren, GuardDuty verwendet AWS Key Management Service (AWS KMS), um die Ergebnisdaten in Ihrem S3-Bucket zu verschlüsseln. Dazu müssen Sie Ihrem S3-Bucket und dem AWS KMS Schlüssel Berechtigungen hinzufügen, damit Sie diese für den Export der Ergebnisse in Ihrem Konto verwenden GuardDuty können.

Inhalt

Überlegungen

Bevor Sie mit den Voraussetzungen und Schritten für den Export von Ergebnissen fortfahren, sollten Sie die folgenden wichtigen Konzepte berücksichtigen:

- Die Exporteinstellungen sind regional — Sie müssen die Exportoptionen in jeder Region, die Sie verwenden, konfigurieren GuardDuty.
- Exportieren von Ergebnissen in Amazon S3 S3-Buckets in verschiedenen AWS-Regionen (regionsübergreifenden) — GuardDuty unterstützt die folgenden Exporteinstellungen:
  - Ihr Amazon S3 S3-Bucket oder Objekt und der AWS KMS Schlüssel müssen zu demselben gehören AWS-Region.
  - Für die in einer Handelsregion generierten Ergebnisse können Sie wählen, ob Sie diese Ergebnisse in einen S3-Bucket in einer beliebigen Handelsregion exportieren möchten. Sie können diese Ergebnisse jedoch nicht in einen S3-Bucket in einer Opt-in-Region exportieren.

  - Für die Ergebnisse, die in einer Opt-in-Region generiert wurden, können Sie wählen, ob Sie diese Ergebnisse in dieselbe Opt-in-Region exportieren möchten, in der sie generiert wurden, oder in eine beliebige kommerzielle Region. Sie können jedoch keine Ergebnisse aus einer Opt-in-Region in eine andere Opt-in-Region exportieren.
- Berechtigungen zum Exportieren von Ergebnissen — Um Einstellungen für den Export aktiver Ergebnisse zu konfigurieren, muss Ihr S3-Bucket über Berechtigungen verfügen, die das Hochladen von GuardDuty Objekten ermöglichen. Sie benötigen außerdem einen AWS KMS Schlüssel, mit dem Sie die Ergebnisse verschlüsseln GuardDuty können.
- Archivierte Ergebnisse werden nicht exportiert — Standardmäßig werden die archivierten Ergebnisse, einschließlich neuer Instanzen unterdrückter Ergebnisse, nicht exportiert.

  Um ein archiviertes Ergebnis zu exportieren, müssen Sie die Archivierung aufheben. Dadurch wird der Status auf Aktiv geändert. Basierend auf der Exporthäufigkeit wird das Ergebnis in den konfigurierten S3-Bucket exportiert.
- GuardDuty Das Administratorkonto kann Ergebnisse exportieren, die in verknüpften Mitgliedskonten generiert wurden — Wenn Sie Exportergebnisse in einem Administratorkonto konfigurieren, werden alle Ergebnisse der zugehörigen Mitgliedskonten, die in derselben Region generiert wurden, auch an denselben Speicherort exportiert, den Sie für das Administratorkonto konfiguriert haben. Weitere Informationen finden Sie unter Grundlegendes zur Beziehung zwischen GuardDuty Administratorkonto und Mitgliedskonten.

Schritt 1 — Für den Export der Ergebnisse sind Berechtigungen erforderlich

Wenn Sie Einstellungen für den Export von Ergebnissen konfigurieren, wählen Sie einen Amazon S3 S3-Bucket aus, in dem Sie die Ergebnisse und einen AWS KMS Schlüssel für die Datenverschlüsselung speichern können. Zusätzlich zu den Berechtigungen für GuardDuty Aktionen müssen Sie auch über Berechtigungen für die folgenden Aktionen verfügen, um die Einstellungen für den Export von Ergebnissen erfolgreich konfigurieren zu können:

- s3: GetBucketLocation
- s3: PutObject

Schritt 2 — Richtlinie an Ihren KMS-Schlüssel anhängen

GuardDuty verschlüsselt die Ergebnisdaten in Ihrem Bucket mithilfe von. AWS Key Management Service Um die Einstellungen erfolgreich zu konfigurieren, müssen Sie zunächst die GuardDuty

Erlaubnis zur Verwendung eines KMS-Schlüssels erteilen. Sie können die Berechtigungen gewähren, indem Sie die Richtlinie an Ihren KMS-Schlüssel anhängen.

Wenn Sie einen KMS-Schlüssel von einem anderen Konto verwenden, müssen Sie die Schlüsselrichtlinie anwenden, indem Sie sich bei dem Konto anmelden AWS-Konto , dem der Schlüssel gehört. Wenn Sie die Einstellungen für den Export von Ergebnissen konfigurieren, benötigen Sie auch den Schlüssel-ARN von dem Konto, dem der Schlüssel gehört.

Um die KMS-Schlüsselrichtlinie für die Verschlüsselung Ihrer exportierten Ergebnisse GuardDuty zu ändern

1. Öffnen Sie die AWS KMS Konsole unter https://console.aws.amazon.com/kms.
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie einen vorhandenen KMS-Schlüssel aus oder führen Sie die Schritte zum Erstellen eines neuen Schlüssels im AWS Key Management Service Entwicklerhandbuch aus, mit dem Sie die exportierten Ergebnisse verschlüsseln werden.

   > **Note**
   >
   > Ihr KMS-Schlüssel und der Amazon S3 S3-Bucket müssen identisch sein. AWS-Region

   Sie können dasselbe S3-Bucket- und KMS-Schlüsselpaar verwenden, um die Ergebnisse aus jeder zutreffenden Region zu exportieren. Weitere Informationen finden Sie unter Informationen Überlegungen zum Exportieren von Ergebnissen zwischen Regionen.
4. Wählen Sie im Abschnitt Key policy (Schlüsselrichtlinie) die Option Edit (Bearbeiten) aus.

   Wenn Zur Richtlinienansicht wechseln angezeigt wird, wählen Sie diese aus, um die Schlüsselrichtlinie anzuzeigen, und klicken Sie dann auf Bearbeiten.
5. Kopieren Sie den folgenden Richtlinienblock in Ihre KMS-Schlüsselrichtlinie, um die GuardDuty Erlaubnis zur Verwendung Ihres Schlüssels zu erteilen.

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
```

```
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "KMS key ARN",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
    }
}
```

6. Bearbeiten Sie die Richtlinie, indem Sie die folgenden Werte ersetzen, die im Richtlinienbeispiel *rot* formatiert sind:

   1. Ersetzen Sie den *KMS-Schlüssel ARN* durch den Amazon-Ressourcennamen (ARN) des KMS-Schlüssels. Informationen zur Suche nach dem Schlüssel-ARN finden Sie unter Suchen der Schlüssel-ID und des ARN im AWS Key Management Service Entwicklerhandbuch.
   2. Ersetzen Sie *123456789012* durch die AWS-Konto ID, der das GuardDuty Konto gehört, das die Ergebnisse exportiert.
   3. Ersetzen Sie *Region2* durch den Ort, an AWS-Region dem die Ergebnisse generiert werden. GuardDuty
   4. Ersetzen Sie *SourceDetectorID* durch die `detectorID` des GuardDuty Accounts in der spezifischen Region, in der die Ergebnisse generiert wurden.

      Die Angabe `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

   > **Note**
   >
   > Wenn Sie GuardDuty in einer Opt-in-Region verwenden, ersetzen Sie den Wert für den „Service“ durch den regionalen Endpunkt für diese Region. Wenn Sie beispielsweise GuardDuty in der Region Naher Osten (Bahrain) (me-south-1) verwenden, ersetzen Sie `"Service": "guardduty.amazonaws.com"` es durch. `"Service": "guardduty.me-south-1.amazonaws.com"` Informationen zu Endpunkten für jede Opt-in-Region finden Sie unter GuardDuty Endpunkte und Kontingente.

7. Wenn Sie die Grundsatzerklärung vor der endgültigen Erklärung hinzugefügt haben, fügen Sie vor dem Hinzufügen dieser Aussage ein Komma hinzu. Stellen Sie sicher, dass die JSON-Syntax Ihrer KMS-Schlüsselrichtlinie gültig ist.

   Wählen Sie Speichern.
8. (Optional) Kopieren Sie den Schlüssel ARN auf einen Notizblock, um ihn in den späteren Schritten zu verwenden.

Schritt 3 — Richtlinie an Amazon S3 S3-Bucket anhängen

Fügen Sie dem Amazon S3 S3-Bucket, in den Sie Ergebnisse exportieren, Berechtigungen hinzu, damit Sie Objekte in diesen S3-Bucket hochladen GuardDuty können. Unabhängig davon, ob Sie einen Amazon S3 S3-Bucket verwenden, der entweder zu Ihrem Konto oder zu einem anderen gehört AWS-Konto, müssen Sie diese Berechtigungen hinzufügen.

Wenn Sie zu irgendeinem Zeitpunkt entscheiden, Ergebnisse in einen anderen S3-Bucket zu exportieren, müssen Sie, um mit dem Export der Ergebnisse fortzufahren, Berechtigungen für diesen S3-Bucket hinzufügen und die Einstellungen für den Export der Ergebnisse erneut konfigurieren.

Wenn Sie noch keinen Amazon S3 S3-Bucket haben, in den Sie diese Ergebnisse exportieren möchten, finden Sie weitere Informationen unter Erstellen eines Buckets im Amazon S3 S3-Benutzerhandbuch.

So fügen Sie Ihrer S3-Bucket-Richtlinie Berechtigungen hinzu

1. Führen Sie die Schritte unter So erstellen oder bearbeiten Sie eine Bucket-Richtlinie im Amazon S3 S3-Benutzerhandbuch aus, bis die Seite Bucket-Richtlinie bearbeiten angezeigt wird.
2. Die Beispielrichtlinie zeigt, wie Sie die GuardDuty Erlaubnis zum Exportieren von Ergebnissen in Ihren Amazon S3 S3-Bucket erteilen. Wenn Sie den Pfad ändern, nachdem Sie Exportergebnisse konfiguriert haben, müssen Sie die Richtlinie ändern, um die Erlaubnis für den neuen Speicherort zu erteilen.

   Kopieren Sie die folgende Beispielrichtlinie und fügen Sie sie in den Bucket-Richtlinieneditor ein.

   Wenn Sie die Richtlinienerklärung vor der endgültigen Aussage hinzugefügt haben, fügen Sie vor dem Hinzufügen dieser Aussage ein Komma hinzu. Stellen Sie sicher, dass die JSON-Syntax Ihrer KMS-Schlüsselrichtlinie gültig ist.

   Beispiel für eine S3-Bucket-Richtlinie

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGuardDutygetBucketLocation",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "Amazon S3 bucket ARN",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "AllowGuardDutyPutObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "DenyUnencryptedUploadsThis is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
```

```
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "DenyIncorrectHeaderThis is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id": "KMS key ARN"
                }
            }
        },
        {
            "Sid": "DenyNon-HTTPS",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

3. Bearbeiten Sie die Richtlinie, indem Sie die folgenden Werte ersetzen, die im Richtlinienbeispiel *rot* formatiert sind:

    1. Ersetzen Sie den *Amazon S3 S3-Bucket-ARN* durch den Amazon-Ressourcennamen (ARN) des Amazon S3-Buckets. Sie finden den Bucket-ARN auf der Seite Bucket-Richtlinie bearbeiten in der https://console.aws.amazon.com/s3/ -Konsole.

2. Ersetzen Sie *123456789012* durch die AWS-Konto ID, der das GuardDuty Konto gehört, das die Ergebnisse exportiert.
3. Ersetzen Sie *Region2* durch den Ort, an AWS-Region dem die Ergebnisse generiert werden. GuardDuty
4. Ersetzen Sie *SourceDetectorID* durch die `detectorID` des GuardDuty Accounts in der spezifischen Region, in der die Ergebnisse generiert wurden.

   Die Angabe `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.
5. Ersetzen Sie den Teil *[optionales Präfix]* des Platzhalterwerts *ARN/ [optionales Präfix] im S3-Bucket* durch einen optionalen Ordnerspeicherort, in den Sie die Ergebnisse exportieren möchten. Weitere Informationen zur Verwendung von Präfixen finden Sie unter Objekte mithilfe von Präfixen organisieren im Amazon S3 S3-Benutzerhandbuch.

   Wenn Sie einen optionalen Ordnerspeicherort angeben, der noch nicht existiert, GuardDuty wird dieser Speicherort nur erstellt, wenn das mit dem S3-Bucket verknüpfte Konto mit dem Konto identisch ist, das die Ergebnisse exportiert. Wenn Sie Ergebnisse in einen S3-Bucket exportieren, der zu einem anderen Konto gehört, muss der Speicherort des Ordners bereits vorhanden sein.
6. Ersetzen Sie den *KMS-Schlüssel ARN* durch den Amazon-Ressourcennamen (ARN) des KMS-Schlüssels, der mit der Verschlüsselung der in den S3-Bucket exportierten Ergebnisse verknüpft ist. Informationen zur Suche nach dem Schlüssel-ARN finden Sie unter Suchen der Schlüssel-ID und des ARN im AWS Key Management Service Entwicklerhandbuch.

> **Note**
>
> Wenn Sie GuardDuty in einer Opt-in-Region verwenden, ersetzen Sie den Wert für den „Service“ durch den regionalen Endpunkt für diese Region. Wenn Sie beispielsweise GuardDuty in der Region Naher Osten (Bahrain) (me-south-1) verwenden, ersetzen Sie `"Service": "guardduty.amazonaws.com"` es durch. `"Service": "guardduty.me-south-1.amazonaws.com"` Informationen zu Endpunkten für jede Opt-in-Region finden Sie unter GuardDuty Endpunkte und Kontingente.

4. Wählen Sie Speichern.

Schritt 4 — Ergebnisse in einen S3-Bucket (Konsole) exportieren

GuardDuty ermöglicht es Ihnen, Ergebnisse in einen vorhandenen Bucket in einem anderen zu exportieren AWS-Konto.

Wenn Sie einen neuen S3-Bucket erstellen oder einen vorhandenen Bucket in Ihrem Konto auswählen, können Sie ein optionales Präfix hinzufügen. GuardDuty Erstellt bei der Konfiguration von Exportergebnissen einen neuen Ordner im S3-Bucket für Ihre Ergebnisse. Das Präfix wird an die von Ihnen GuardDuty erstellte Standardordnerstruktur angehängt. Zum Beispiel das Format des optionalen Präfixes`AWSLogs/`*`123456789012`*`/GuardDuty/`*`Region`*.

Der gesamte Pfad des S3-Objekts wird sein*`DOC-EXAMPLE-BUCKET`*`/`*`prefix-name`*`/UUID`*`.jsonl.gz`*. Das `UUID` wird zufällig generiert und stellt weder die Melder-ID noch die Befund-ID dar.

> **Important**
>
> Der KMS-Schlüssel und der S3-Bucket müssen sich in derselben Region befinden.

Bevor Sie diese Schritte ausführen, stellen Sie sicher, dass Sie Ihrem KMS-Schlüssel und Ihrem vorhandenen S3-Bucket die entsprechenden Richtlinien angehängt haben.

Um Exportergebnisse zu konfigurieren

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie auf der Seite Einstellungen unter Exportoptionen für Ergebnisse für den S3-Bucket die Option Jetzt konfigurieren (oder je nach Bedarf Bearbeiten) aus.
4. Geben Sie für den S3-Bucket ARN den ein**`bucket ARN`**. Informationen zum Bucket ARN finden Sie unter Eigenschaften für einen S3-Bucket anzeigen im Amazon S3 S3-Benutzerhandbuch. Auf der Registerkarte „Berechtigungen“ auf der Eigenschaftenseite des zugehörigen Buckets in der https://console.aws.amazon.com/guardduty/ -Konsole.
5. Geben Sie für KMS-Schlüssel-ARN den ein **`key ARN`**. Informationen zur Suche nach dem Schlüssel-ARN finden Sie unter Suchen der Schlüssel-ID und des ARN im AWS Key Management Service Entwicklerhandbuch.

6. Richtlinien anhängen

   - Führen Sie die Schritte aus, um die S3-Bucket-Richtlinie anzuhängen. Weitere Informationen finden Sie unter Schritt 3 — Richtlinie an Amazon S3 S3-Bucket anhängen.

   - Führen Sie die Schritte aus, um die KMS-Schlüsselrichtlinie anzuhängen. Weitere Informationen finden Sie unter Schritt 2 — Richtlinie an Ihren KMS-Schlüssel anhängen.

7. Wählen Sie Save (Speichern) aus.

Schritt 5 — Einstellung der Häufigkeit für den Export aktualisierter aktiver Ergebnisse

Konfigurieren Sie die Häufigkeit für den Export aktualisierter aktiver Ergebnisse entsprechend Ihrer Umgebung. Standardmäßig werden aktualisierte Ergebnisse alle 6 Stunden exportiert. Dies bedeutet, dass alle Ergebnisse in den nächsten Export aufgenommen werden, die nach dem letzten Export aktualisiert wurden. Wenn aktualisierte Ergebnisse alle 6 Stunden exportiert werden und dieser Export um 12:00 Uhr erfolgt, wird jedes nach 12:00 Uhr aktualisierte Ergebnis um 18:00 Uhr exportiert.

So stellen Sie die Häufigkeit ein

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie im Bereich Exportoptionen für Erkenntnisse die Option Häufigkeit für aktualisierte Erkenntnisse aus. Dadurch wird die Häufigkeit für den Export aktualisierter Active-Ergebnisse EventBridge sowohl nach Amazon S3 als auch nach Amazon S3 festgelegt. Sie können aus den folgenden Optionen auswählen:

   - Update EventBridge und S3 alle 15 Minuten
   - Update EventBridge und S3 alle 1 Stunde
   - Update CWE and S3 every 6 hours (default) (Aktualisieren von CWE und S3 alle 6 Stunden (Standard))

4. Wählen Sie Save Changes.

Erstellen von benutzerdefinierten Antworten auf GuardDuty Erkenntnisse mit Amazon CloudWatch Events

GuardDuty erstellt ein Ereignis für Amazon CloudWatch Events, wenn eine Änderung der Ergebnisse stattfindet. Zu den Erkenntnissen, die ein CloudWatch Ereignis erstellen, gehören neu generierte Erkenntnisse oder neu aggregierte Erkenntnisse. Ereignisse werden auf bestmögliche Weise ausgegeben.

Jedem GuardDuty Ergebnis wird eine Erkenntnis-ID zugewiesen. GuardDuty erstellt ein CloudWatch Ereignis für jedes Ergebnis mit einer eindeutigen Erkenntnis-ID. Jegliches nachfolgendes Vorkommen eines vorhandenen Ergebnisses wird zu den ursprünglichen Ergebnissen aggregiert. Weitere Informationen finden Sie unter GuardDuty Aggregation finden.

> **Note**
>
> Wenn Ihr Konto ein GuardDuty delegierter Administrator ist, werden die CloudWatch Ereignisse in Ihrem Konto sowie in dem Mitgliedskonto veröffentlicht, in dem die Erkenntnis generiert wurde.

Durch die Verwendung von CloudWatch Ereignissen mit können Sie Aufgaben automatisieren GuardDuty, um auf Sicherheitsprobleme zu reagieren, die durch GuardDuty Erkenntnisse aufgedeckt werden.

Um Benachrichtigungen über GuardDuty Erkenntnisse basierend auf CloudWatch Ereignissen zu erhalten, müssen Sie eine CloudWatch Ereignisregel und ein Ziel für erstellen GuardDuty. Diese Regel ermöglicht CloudWatch es , Benachrichtigungen für Erkenntnisse zu senden, die an das in der Regel angegebene Ziel GuardDuty generiert. Weitere Informationen finden Sie unter Erstellen einer CloudWatch Ereignisregel und eines Ziels für GuardDuty (CLI).

Themen

CloudWatch Häufigkeit der Ereignisbenachrichtigung für GuardDuty

Benachrichtigungen für neu generierte Erkenntnisse mit einer eindeutigen Erkenntnis-ID

GuardDuty sendet innerhalb von 5 Minuten nach dem Ergebnis eine Benachrichtigung basierend auf seinem CloudWatch Ereignis. Dieses Ereignis (und diese Benachrichtigung) beinhalten auch alle nachfolgenden Vorkommen dieses Ergebnisses, die innerhalb der ersten 5 Minuten seit der Generierung dieses Ergebnisses mit einer eindeutigen ID stattfinden.

> **Note**
>
> Die Häufigkeit der Benachrichtigungen über neu erstellte Erkenntnisse beträgt standardmäßig 5 Minuten. Diese Frequenz kann nicht aktualisiert werden.

Benachrichtigungen für nachfolgende Erkenntnisse

Standardmäßig GuardDuty aggregiert für jede Erkenntnis mit einer eindeutigen Erkenntnis-ID alle nachfolgenden Vorkommen eines bestimmten Erkenntnistyps, die innerhalb der 6-Stunden-Intervalle stattfinden, in einem einzigen Ereignis. GuardDuty sendet dann basierend auf diesem Ereignis eine Benachrichtigung über diese nachfolgenden Vorkommen. Standardmäßig GuardDuty sendet für die nachfolgenden Vorkommen der vorhandenen Erkenntnisse alle 6 Stunden Benachrichtigungen basierend auf CloudWatch Ereignissen.

Nur ein Administratorkonto kann die Standardhäufigkeit der Benachrichtigungen anpassen, die über die nachfolgenden Erkenntnisereignisse an CloudWatch Ereignisse gesendet werden. Benutzer von Mitgliedskonten können diesen Häufigkeitswert nicht anpassen. Der vom Administratorkonto in seinem eigenen Konto festgelegte Häufigkeitswert wird der GuardDuty Funktionalität in allen seinen Mitgliedskonten auferlegt. Wenn ein Benutzer aus einem Administratorkonto diesen Häufigkeitswert auf 1 Stunde festlegt, haben alle Mitgliedskonten auch die Häufigkeit von 1 Stunde, mit der Benachrichtigungen über die nachfolgenden Erkenntnisereignisse empfangen werden. Weitere Informationen finden Sie unter Verwaltung mehrerer Konten bei Amazon GuardDuty.

> **Note**
>
> Als Administratorkonto können Sie die Standardhäufigkeit von Benachrichtigungen über die nachfolgenden Erkenntnisereignisse anpassen. Mögliche Werte sind 15 Minuten,

1 Stunde oder standardmäßig 6 Stunden. Weitere Informationen zum Einrichten der Häufigkeit für diese Benachrichtigungen finden Sie unter Schritt 5 — Einstellung der Häufigkeit für den Export aktualisierter aktiver Ergebnisse.

Überwachen archivierter GuardDuty Ergebnisse mit - CloudWatch Ereignissen

Für die manuell archivierten Erkenntnisse werden die ersten und alle nachfolgenden Vorkommen dieser Erkenntnisse (die nach Abschluss der Archivierung generiert wurden) mit der oben beschriebenen Häufigkeit an CloudWatch Ereignisse gesendet.

Bei den automatisch archivierten Erkenntnissen werden das anfängliche und alle nachfolgenden Vorkommen dieser Erkenntnisse (die nach Abschluss der Archivierung generiert wurden) nicht an CloudWatch Ereignisse gesendet.

CloudWatch Ereignisformat für GuardDuty

Das CloudWatch Ereignis für GuardDuty hat das folgende Format.

```
{
 "version": "0",
 "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
 "detail-type": "GuardDuty Finding",
 "source": "aws.guardduty",
 "account": "111122223333",
 "time": "1970-01-01T00:00:00Z",
 "region": "us-east-1",
 "resources": [],
 "detail": {GUARDDUTY_FINDING_JSON_OBJECT}
}
```

Note

Der Detailwert gibt die JSON-Details einer einzelnen Erkenntnis als Objekt zurück, im Gegensatz zum Wert „Erkenntnisse“, der mehrere Erkenntnisse innerhalb eines Arrays unterstützen kann.

Eine vollständige Liste aller Parameter in der `GUARDDUTY_FINDING_JSON_OBJECT` finden Sie unter GetFindings. Der `id`-Parameter, der in der `GUARDDUTY_FINDING_JSON_OBJECT` angezeigt wird, ist die zuvor beschriebene Ergebnis-ID.

Erstellen einer CloudWatch Ereignisregel, um Sie über GuardDuty Ergebnisse zu informieren (Konsole)

Sie können CloudWatch Ereignisse mit verwenden GuardDuty , um automatische Erkennungswarnungen einzurichten, indem Sie Erkenntnisereignisse an einen Messaging-Hub senden GuardDuty, um die Sichtbarkeit von GuardDuty Erkenntnissen zu erhöhen. In diesem Thema erfahren Sie, wie Sie Ergebniswarnungen an E-Mail, Slack oder Amazon Chime senden, indem Sie ein SNS-Thema einrichten und dieses Thema dann mit einer CloudWatch Ereignisregel für Ereignisse verbinden.

Einrichten eines Amazon-SNS-Themas und eines Endpunkts

Zu Beginn müssen Sie zunächst ein Thema in Amazon Simple Notification Service einrichten und einen Endpunkt hinzufügen. Weitere Informationen dazu erhalten Sie unter Erste Schritte im Entwicklerhandbuch für Amazon Simple Notification Service.

Dieses Verfahren legt fest, wohin Sie GuardDuty Erkenntnisdaten senden möchten. Das SNS-Thema kann während oder nach der Erstellung der Ereignisregel zu einer CloudWatch Ereignisereignisregel hinzugefügt werden.

Email setup

Erstellen eines SNS-Themas

1. Melden Sie sich bei der Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home an.
2. Wählen Sie im Navigationsbereich Topics (Themen) und dann Create Topic (Thema erstellen) aus.
3. Wählen Sie im Abschnitt Thema erstellen die Option Standard. Geben Sie einen Namen für das Thema ein (z. B. **`GuardDuty_to_Email`**). Weitere Angaben sind optional.
4. Wählen Sie Create Topic (Thema erstellen) aus. Die Themeneinzelheiten für Ihr neues Thema werden geöffnet.
5. Wählen Sie im Abschnitt „Subscriptions (Abonnements)“ die Option Create subscription (Abonnement erstellen) aus.

6. a. Wählen Sie im Menü Protocol (Protokoll) die Option Email (E-Mail) aus.

   b. Fügen Sie im Feld Endpoint (Endpunkt) die E-Mail-Adresse hinzu, an der Sie Benachrichtigungen erhalten möchten.

   > **Note**
   >
   > Sie werden aufgefordert, Ihr Abonnement über Ihren E-Mail-Client zu bestätigen, nachdem Sie es erstellt haben.

   c. Wählen Sie Abonnement erstellen.

7. Suchen Sie in Ihrem Posteingang nach einer Abonnementnachricht und wählen Sie Confirm Subscription (Abonnement bestätigen) aus.

Slack setup

Erstellen eines SNS-Themas

1. Melden Sie sich bei der Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home an.
2. Wählen Sie im Navigationsbereich Topics (Themen) und dann Create Topic (Thema erstellen) aus.
3. Wählen Sie im Abschnitt Thema erstellen die Option Standard. Geben Sie einen Namen für das Thema ein (z. B. **`GuardDuty_to_Slack`**). Weitere Angaben sind optional. Wählen Sie Thema erstellen, um den Vorgang abzuschließen.

Konfigurieren eines AWS Chatbot-Clients

1. Navigieren Sie zur AWS Chatbot-Konsole.
2. Wählen Sie im Bereich Konfigurierte Clients die Option Neuen Client konfigurieren.
3. Wählen Sie Slack und bestätigen Sie mit „Konfigurieren“.

> **Note**
>
> Bei der Auswahl von Slack müssen Sie die Zugriffsrechte für AWS Chatbot für Ihren Kanal bestätigen, indem Sie „Zulassen“ wählen.

4. Wählen Sie Neuen Kanal konfigurieren aus, um den Bereich mit den Konfigurationsdetails zu öffnen.

   a. Geben Sie einen Namen für den Kanal ein.

   b. Wählen Sie für den Slack-Kanal den Kanal, den Sie verwenden möchten. Um den privaten Slack-Kanal mit AWS Chatbot zu verwenden, wählen Sie „Privater Kanal“.

   c. Kopieren Sie in Slack die Kanal-ID des privaten Kanals, indem Sie mit der rechten Maustaste auf den Kanalnamen klicken und „Link kopieren“ wählen.

   d. Fügen Sie in der AWS-Verwaltungskonsole im AWS Chatbot-Fenster die ID, die Sie aus Slack kopiert haben, in das Feld Privatkanal-ID ein.

   e. Wählen Sie unter Berechtigungen, ob Sie eine IAM-Rolle mithilfe einer Vorlage erstellen möchten, falls Sie noch keine Rolle haben.

   f. Wählen Sie in Richtlinienvorlagen die Option „Benachrichtigungs-Berechtigungen“ aus. Dies ist die IAM-Richtlinienvorlage für AWS Chatbot. Es bietet die erforderlichen Lese- und Listenberechtigungen für CloudWatch Alarme, Ereignisse und Protokolle sowie für Amazon SNS-Themen.

   g. Wählen Sie die Region aus, in der Sie zuvor Ihr SNS-Thema erstellt haben, und wählen Sie dann das Amazon-SNS-Thema aus, das Sie erstellt haben, um Benachrichtigungen an den Slack-Kanal zu senden.

5. Wählen Sie Konfigurieren.

Chime setup

Erstellen eines SNS-Themas

1. Melden Sie sich bei der Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home an.
2. Wählen Sie im Navigationsbereich Topics (Themen) und dann Create Topic (Thema erstellen) aus.
3. Wählen Sie im Abschnitt Thema erstellen die Option Standard. Geben Sie einen Namen für das Thema ein (z. B. **`GuardDuty_to_Chime`**). Weitere Angaben sind optional. Wählen Sie Thema erstellen, um den Vorgang abzuschließen.

Konfigurieren eines AWS Chatbot-Clients

1. Navigieren Sie zur AWS Chatbot-Konsole.
2. Wählen Sie im Bereich Konfigurierte Clients die Option Neuen Client konfigurieren.
3. Wählen Sie „Chime“ und bestätigen Sie mit „Konfigurieren“.
4. Geben Sie im Bereich mit den Konfigurationsdetails einen Namen für den Kanal ein.
5. Öffnen Sie in Chime den gewünschten Chatraum
    a. Wählen Sie das Zahnradsymbol rechts oben und danach Manage webhooks and bots aus.
    b. Wählen Sie URL kopieren, um die Webhook-URL in Ihre Zwischenablage zu kopieren.
6. Fügen Sie in der AWS-Verwaltungskonsole im AWS Chatbot-Fenster die URL, die Sie kopiert haben, in das Feld Webhook-URL ein.
7. Wählen Sie unter Berechtigungen, ob Sie eine IAM-Rolle mithilfe einer Vorlage erstellen möchten, falls Sie noch keine Rolle haben.
8. Wählen Sie in Richtlinienvorlagen die Option „Benachrichtigungs-Berechtigungen“ aus. Dies ist die IAM-Richtlinienvorlage für AWS Chatbot. Es bietet die erforderlichen Lese- und Listenberechtigungen für CloudWatch Alarme, Ereignisse und Protokolle sowie für Amazon SNS-Themen.
9. Wählen Sie die Region aus, in der Sie zuvor Ihr SNS-Thema erstellt haben, und wählen Sie dann das Amazon-SNS-Thema aus, das Sie erstellt haben, um Benachrichtigungen an den Chime-Raum zu senden.
10. Wählen Sie Konfigurieren.

Einrichten eines CloudWatch Ereignisses für GuardDuty Ergebnisse

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Rules (Regeln) und dann Create Rule (Regel erstellen) aus.
3. Wählen Sie im Menü Servicename die Option ausGuardDuty.
4. Wählen Sie im Menü Ereignistyp die Option GuardDuty Suchen aus.
5. Wählen Sie neben Event Pattern Preview (Vorversion des Ereignismusters) die Option Edit (Bearbeiten) aus.
6. Fügen Sie den folgenden JSON-Code in die Event Pattern Preview (Vorversion des Ereignismusters) ein und wählen Sie Save (Speichern) aus

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "severity": [
      4,
      4.0,
      4.1,
      4.2,
      4.3,
      4.4,
      4.5,
      4.6,
      4.7,
      4.8,
      4.9,
      5,
      5.0,
      5.1,
      5.2,
      5.3,
      5.4,
      5.5,
      5.6,
      5.7,
      5.8,
      5.9,
      6,
      6.0,
      6.1,
      6.2,
      6.3,
      6.4,
      6.5,
      6.6,
      6.7,
      6.8,
      6.9,
      7,
```

```
      7.0,
      7.1,
      7.2,
      7.3,
      7.4,
      7.5,
      7.6,
      7.7,
      7.8,
      7.9,
      8,
      8.0,
      8.1,
      8.2,
      8.3,
      8.4,
      8.5,
      8.6,
      8.7,
      8.8,
      8.9
    ]
  }
}
```

> **Note**
>
> Der obige Code warnt bei jedem Ergebnis der mittleren bis hohen Stufe.

7. Klicken Sie im Abschnitt Targets (Ziele) auf Add Target (Ziel hinzufügen).
8. Wählen Sie im Menü Select Targets (Ziele auswählen) die Option SNS Topic (SNS-Thema) aus.
9. Wählen Sie unter Select Topic (Thema auswählen) den Namen des SNS-Themas aus, das Sie in Schritt 1 erstellt haben.
10. Konfigurieren Sie die Eingabe für das Ereignis.

    - Wenn Sie Benachrichtigungen für Chime oder Slack einrichten, fahren Sie mit Schritt 11 fort, denn der Eingabetyp ist standardmäßig Abgestimmtes Ereignis.
    - Wenn Sie Benachrichtigungen für E-Mails über SNS einrichten, führen Sie die folgenden Schritte aus, um die an Ihren Posteingang gesendete Nachricht anzupassen:

a. Erweitern Sie Configure input (Eingabe konfigurieren) und wählen Sie dann Input Transformer (Eingabetransformer) aus.

b. Kopieren Sie den folgenden Code und fügen Sie ihn in das Feld Input Path (Eingabepfad) ein.

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

c. Kopieren Sie den folgenden Code und fügen Sie ihn in das Feld Input Template (Eingabevorlage) ein, um die E-Mail zu formatieren.

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type
 <Finding_Type> in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id%3D<Finding_ID>"
```

11. Klicken Sie auf Configure Details (Details konfigurieren).
12. Geben Sie auf der Seite Configure rule details (Regeldetails konfigurieren) einen Name (Name) und eine Description (Beschreibung) für die Regel ein und wählen Sie dann Create Rule (Regel erstellen) aus.

Erstellen einer CloudWatch Ereignisregel und eines Ziels für GuardDuty (CLI)

Das folgende Verfahren zeigt, wie Sie -AWS CLIBefehle verwenden, um eine CloudWatch Ereignisregel und ein Ziel für zu erstellen GuardDuty. Insbesondere zeigt Ihnen das Verfahren, wie

Sie eine Regel erstellen, die es ermöglicht, Ereignisse für alle Erkenntnisse CloudWatch zu senden, die GuardDuty generiert, und eine -AWS LambdaFunktion als Ziel für die Regel hinzuzufügen.

> **Note**
>
> Zusätzlich zu den Lambda-Funktionen GuardDuty und CloudWatch unterstützen die folgenden Zieltypen: Amazon EC2-Instances, Amazon Kinesis-Streams, Amazon-ECS-Aufgaben, AWS Step Functions Zustandsautomaten, den `-run`Befehl und integrierte Ziele.

Sie können auch eine CloudWatch Ereignisregel und ein Ziel für GuardDuty über die CloudWatch Ereigniskonsole erstellen. Weitere Informationen und detaillierte Schritte finden Sie unter Erstellen einer CloudWatch Ereignisregel, die bei einem Ereignis ausgelöst wird. Wählen Sie im Abschnitt Event Source **`GuardDuty`** für Service name und **`GuardDuty Finding`** für Event Type aus.

Erstellen von Regeln und Zielen

1. Führen Sie den folgenden CloudWatch CLI-Befehl aus, um eine Regel CloudWatch zu erstellen, die GuardDuty das Senden von Ereignissen für alle von generierten Erkenntnisse ermöglicht.

   ```
   AWS events put-rule --name Test --event-pattern "{\"source\":
   [\"aws.guardduty\"]}"
   ```

   > **Important**
   >
   > Sie können Ihre Regel weiter anpassen, sodass sie anweist CloudWatch , Ereignisse nur für eine Teilmenge der von generierten Erkenntnisse GuardDutyzu senden. Diese Untergruppe basiert auf dem/den in der Regel angegebenen Ergebnisattribut(en). Verwenden Sie beispielsweise den folgenden CLI-Befehl, um eine Regel zu erstellen, die es ermöglicht CloudWatch , nur Ereignisse für die GuardDuty Ergebnisse mit dem Schweregrad 5 oder 8 zu senden:
   > ```
   > AWS events put-rule --name Test --event-pattern "{\"source\":
   > [\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"],
   > \"detail\":{\"severity\":[5,8]}}"
   > ```
   > Zu diesem Zweck können Sie jeden der Eigenschaftswerte verwenden, die im JSON für GuardDuty Ergebnisse verfügbar sind.

2. Um eine Lambda-Funktion als Ziel für die Regel anzufügen, die Sie in Schritt 1 erstellt haben, führen Sie den folgenden CloudWatch CLI-Befehl aus.

   ```
   AWS events put-targets --rule Test --targets
   Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
   ```

   > **Note**
   >
   > Stellen Sie sicher, dass Sie <your_function> im obigen Befehl durch Ihre tatsächliche Lambda-Funktion für die GuardDuty Ereignisse ersetzen.

3. Führen Sie den folgenden Lambda-CLI-Befehl aus, um die erforderlichen Berechtigungen zum Aufrufen des Ziels hinzuzufügen.

   ```
   AWS lambda add-permission --function-name <your_function> --statement-
   id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
   ```

   > **Note**
   >
   > Stellen Sie sicher, dass Sie <your_function> im obigen Befehl durch Ihre tatsächliche Lambda-Funktion für die GuardDuty Ereignisse ersetzen.

   > **Note**
   >
   > Im obigen Verfahren verwenden wir eine Lambda-Funktion als Ziel für die Regel, die CloudWatch Ereignisse auslöst. Sie können auch andere AWS Ressourcen als Ziele konfigurieren, um CloudWatch Ereignisse auszulösen. Weitere Informationen finden Sie unter PutTargets.

CloudWatch Ereignisse für Umgebungen mit GuardDuty mehreren Konten

Als GuardDuty Administrator werden CloudWatch Ereignisregeln in Ihrem Konto basierend auf den entsprechenden Erkenntnissen aus Ihren Mitgliedskonten ausgelöst. Das bedeutet, dass Sie, wenn Sie über CloudWatch Ereignisse in Ihrem Administratorkonto, wie im vorherigen Abschnitt beschrieben, eine Benachrichtigung über Erkenntnisse mit hohem und mittlerem Schweregrad einrichten, die von Ihren Mitgliedskonten zusätzlich zu Ihren eigenen generiert werden.

Sie können das Mitgliedskonto, von dem die GuardDuty Erkenntnis stammt, mit dem `accountId` Feld der JSON-Details der Erkenntnis identifizieren.

Um mit dem Schreiben einer benutzerdefinierten Ereignisregel für ein bestimmtes Mitgliedskonto in Ihrer Umgebung in der Konsole zu beginnen, erstellen Sie eine neue Regel und fügen Sie die folgende Vorlage in die Ereignismustervorschau ein. Fügen Sie dabei die Konto-ID des Mitgliedskontos hinzu, das das Ereignis auslösen soll.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

> **Note**
>
> Dieses Beispiel wird bei allen Erkenntnissen für die angegebene Konto-ID ausgelöst. Gemäß der JSON-Syntax können mehrere IDs hinzugefügt werden, die durch ein Komma getrennt sind.

Grundlegendes zu CloudWatch Protokollen und Gründen für das Überspringen von Ressourcen beim Malware-Schutz-Scan

GuardDuty Malware Protection veröffentlicht Ereignisse in Ihrer CloudWatch Amazon-Protokollgruppe /aws/guardduty/ malware-scan-events. Für jedes Ereignis im Zusammenhang mit dem Malware-Scan können Sie den Status und das Scanergebnis Ihrer betroffenen Ressourcen überwachen. Bestimmte Amazon-EC2-Ressourcen und Amazon-EBS-Volumes wurden möglicherweise während des Malware-Protection-Scans übersprungen.

GuardDuty Protokolle im CloudWatch Malware-Schutz prüfen

In der Protokollgruppe /aws/guardduty/ malware-scan-events CloudWatch werden drei Arten von Scanereignissen unterstützt.

Name des Scanereignisses von Malware Protection	Erklärung
`EC2_SCAN_STARTED`	Wird erstellt, wenn ein GuardDuty Malware-Schutz den Prozess des Malware-Scans einleitet, z. B. die Erstellung eines Snapshots eines EBS-Volumes vorbereitet.
`EC2_SCAN_COMPLETED`	Wird erstellt, wenn der GuardDuty Malware-Schutz-Scan für mindestens eines der EBS-Volumes der betroffenen Ressource abgeschlossen ist. Dieses Ereignis umfasst auch das `snapshotId`, das zum gescannten EBS-Volume gehört. Nach Abschluss des Scans lautet das Scanergebnis entweder `CLEAN`, `THREATS_FOUND` oder `NOT_SCANNED`.
`EC2_SCAN_SKIPPED`	Wird erstellt, wenn der GuardDuty Malware-Schutz-Scan alle EBS-Volumes der betroffenen Ressource überspringt. Um den Grund für das Überspringen zu ermitteln, wählen Sie das entsprechende Ereignis aus und sehen Sie sich die Details an. Weitere Informationen zu den Gründen für das Überspringen finden Sie unter Gründe für das Überspringen von Ressourcen beim Malware-Scan weiter unten.

> **Note**
>
> Wenn Sie eine verwenden AWS Organizations, werden CloudWatch Protokollereignisse von Mitgliedskonten in Organizations sowohl im Administratorkonto als auch in der Protokollgruppe des Mitgliedskontos veröffentlicht.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um CloudWatch Ereignisse anzuzeigen und abzufragen.

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Protokolle die Option Protokollgruppen. Wählen Sie die malware-scan-events Protokollgruppe /aws/guardduty/, um die Scanereignisse für den Malware-Schutz anzuzeigen. GuardDuty

   Um eine Abfrage auszuführen, wählen Sie Log Insights.

   Informationen zum Ausführen einer Abfrage finden Sie unter Analysieren von Protokolldaten mit CloudWatch Logs Insights im CloudWatch Amazon-Benutzerhandbuch.
3. Wählen Sie Scan-ID, um die Details der betroffenen Ressourcen und Malware-Erkenntnisse zu überwachen. Sie können beispielsweise die folgende Abfrage ausführen, um die CloudWatch Protokollereignisse zu filtern, indem Sie`scanId`. Stellen Sie sicher, dass Sie Ihre eigene gültige *`Scan-ID`* verwenden.

   ```
   fields @timestamp, @message, scanRequestDetails.scanId as scanId
   | filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
   | sort @timestamp asc
   ```

API/CLI

- Informationen zur Arbeit mit Protokollgruppen finden Sie unter Suchen nach Protokolleinträgen mithilfe von AWS CLI im CloudWatch Amazon-Benutzerhandbuch.

  Wählen Sie die malware-scan-events Protokollgruppe /aws/guardduty/, um die Scan-Ereignisse für den Malware-Schutz anzuzeigen. GuardDuty

- Informationen zum Anzeigen und Filtern von Protokollereignissen finden Sie unter GetLogEventsbzw. in der Amazon CloudWatch API-Referenz. FilterLogEvents

GuardDuty Aufbewahrung von Malware-Schutz-Protokollen

Die standardmäßige Aufbewahrungsfrist für die Protokollgruppe /aws/guardduty/ beträgt 90 Tage. Danach werden die malware-scan-events Protokollereignisse automatisch gelöscht. Informationen zum Ändern der Protokollaufbewahrungsrichtlinie für Ihre Protokollgruppe finden Sie unter Ändern der Aufbewahrung von CloudWatch Protokolldaten in Logs oder. CloudWatch PutRetentionPolicy

Gründe für das Überspringen von Ressourcen beim Malware-Scan

Bei Ereignissen im Zusammenhang mit dem Malware-Scan wurden möglicherweise bestimmte EC2-Ressourcen und EBS-Volumes während des Scanvorgangs übersprungen. In der folgenden Tabelle sind die Gründe aufgeführt, warum GuardDuty Malware Protection die Ressourcen möglicherweise nicht scannt. Verwenden Sie gegebenenfalls die vorgeschlagenen Schritte, um diese Probleme zu beheben, und scannen Sie diese Ressourcen, wenn der GuardDuty Malware-Schutz das nächste Mal einen Malware-Scan einleitet. Die anderen Probleme dienen dazu, Sie über den Verlauf der Ereignisse zu informieren, und sind nicht umsetzbar.

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte	
`RESOURCE_NOT_FOUND`	Der `resourceArn` zur Initiierung des On-Demand-Scans bereitgestellte Malware-Scan wurde in Ihrer AWS Umgebung nicht gefunden.	Überprüfen Sie den `resourceArn` Ihres Amazon-EC2-Instance- oder Container-Workloads und versuchen Sie es erneut.	
`ACCOUNT_INELIGIBLE`	Die AWS Konto-ID, von der aus Sie versucht haben, einen On-Demand-Malware-Scan zu starten,	Stellen Sie sicher, dass GuardDuty es für dieses AWS Konto aktiviert ist.	

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte	
	wurde nicht aktiviert GuardDuty.	Wenn Sie ein neues Konto aktivieren GuardDuty AWS-Region , kann die Synchronisierung bis zu 20 Minuten dauern.	
`UNSUPPORTED_KEY_ENCRYPTION`	GuardDuty Malware Protection unterstützt Volumes, die sowohl unverschlüsselt als auch mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind. Das Scannen von EBS-Volumes, die mit der Amazon-EBS-Verschlüsselung verschlüsselt wurden, wird nicht unterstützt. Derzeit gibt es einen regionalen Unterschied, bei dem dieser Übersprungsgrund nicht zutrifft. Weitere Informationen zu diesen finden Sie AWS-Regionen unterVerfügbarkeit regionsspezifischer Feature.	Ersetzen Sie Ihren Verschlüsselungsschlüssel durch einen vom Kunden verwalteten Schlüssel. Weitere Informationen zu den GuardDuty unterstützten Verschlüsselungsarten finden Sie unterUnterstützte Amazon EBS-Volumes für Malware-Scans.	

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte	
`EXCLUDED_BY_SCAN_SETTINGS`	Die EC2-Instance oder das EBS-Volume wurde beim Malware-Scan ausgeschlossen. Es gibt zwei Möglichkeiten: Entweder wurde das Tag zur Einschließen-Liste hinzugefügt, aber die Ressource ist nicht mit diesem Tag verknüpft, das Tag wurde der Ausschließen-Liste hinzugefügt und die Ressource ist mit diesem Tag verknüpft, oder das `GuardDuty Excluded` -Tag ist für diese Ressource auf `true` gesetzt.	Aktualisieren Sie Ihre Scan-Optionen oder die Ihrer Amazon-EC2-Ressource zugeordneten Tags. Weitere Informationen finden Sie unter Scan-Optionen mit benutzerdefinierten Tags.	
`UNSUPPORTED_VOLUME_SIZE`	Das Volumen ist größer als 2048 GB.	Nicht umsetzbar.	
`NO_VOLUMES_ATTACHED`	GuardDuty Der Malware-Schutz hat die Instance in Ihrem Konto gefunden, aber es wurde kein EBS-Volume an diese Instance angehängt, um mit dem Scan fortzufahren.	Nicht umsetzbar.	

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte	
UNABLE_TO_SCAN	Es ist ein interner Servicefehler.	Nicht umsetzbar.	
SNAPSHOT_NOT_FOUND	Die von den EBS-Volumes erstellten und mit dem Dienstkonto geteilten Snapshots wurden nicht gefunden, und GuardDuty Malware Protection konnte den Scan nicht fortsetzen.	Stellen CloudTrail Sie sicher, dass die Snapshots nicht absichtlich entfernt wurden.	
SNAPSHOT_QUOTA_REACHED	Sie haben das maximale Volumen erreicht, das für Snapshots für jede Region zulässig ist. Dadurch wird verhindert, dass Snapshots nicht nur gespeichert, sondern auch neue erstellt werden.	Sie können entweder alte Snapshots entfernen oder eine Erhöhung des Kontingents beantragen. Das Standardlimit für Snapshots pro Region und wie Sie eine Erhöhung des Kontingents beantragen können, finden Sie unter Service Quotas im Allgemeinen Referenzhandbuch von AWS .	

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte	
`MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED`	Mehr als 11 EBS-Volumes wurden an eine EC2-Instance angehängt. GuardDuty Malware Protection hat die ersten 11 EBS-Volumes gescannt, die durch alphabetische Sortierung ermittelt wurden. `deviceName`	Nicht umsetzbar.	
`UNSUPPORTED_PRODUCT_CODE_TYPE`	GuardDuty unterstützt das Scannen von Instances mit `productCode` as nicht. `marketplace` Weitere Informationen finden Sie unter Bezahlte AMIs im Amazon-EC2-Benutzerhandbuch für Linux-Instances. Weitere Informationen zu `productCode` finden Sie unter ProductCode in der Amazon-EC2-API-Referenz.	Nicht umsetzbar.	

Falschmeldungen in GuardDuty Malware Protection melden

Scans von GuardDuty Malware Protection können eine harmlose Datei in Ihrer Amazon-EC2-Instance oder Ihrem Container-Workload als bösartig oder schädlich identifizieren. Um Ihre Erfahrung mit dem Malware Protection und dem GuardDuty-Service zu verbessern, können Sie falsch positive Ergebnisse melden, wenn Sie der Meinung sind, dass eine Datei, die während eines Scans als bösartig oder schädlich identifiziert wurde, tatsächlich keine Malware enthält.

Falsch positive Dateiübermittlung

1. Melden Sie sich in der https://console.aws.amazon.com/guardduty/-Konsole an.
2. Wenn Sie feststellen, dass es sich um ein scheinbar falsch positives Ergebnis handelt, wenden Sie sich an AWS Support, um den Prozess der Einreichung einer falsch positiven Datei einzuleiten.
3. Wählen Sie Malware-Scans.
4. Wählen Sie einen Scan aus, um die zugehörige Erkenntnis-ID anzuzeigen.
5. Geben Sie die Erkenntnis-ID ein. Sie müssen auch den SHA-256-Hashwert der Datei angeben. Dies ist erforderlich, um sicherzustellen, dass GuardDuty Malware Protection die richtige Datei erhalten hat.
6. Das AWS Support-Team stellt Ihnen eine Amazon Simple Storage Service (S3)-URL zur Verfügung, mit der Sie die Datei und den SHA-256-Hash hochladen können. Informieren Sie das AWS Support-Team, nachdem Sie die Datei erfolgreich hochgeladen haben.

   > **Warning**
   >
   > Übergeben Sie die Datei oder den SHA-256-Hash nicht direkt an AWS Support.
   > Sie sollten die Datei und den Hash nur über die angegebene URL auf Amazon S3 hochladen. Wenn Sie die Datei und den Hash nicht innerhalb von sieben Tagen nach Erhalt der URL hochladen, werden sie ungültig. Wenn die URL ungültig wird, müssen Sie sich an AWS Support wenden, um eine neue URL zu erhalten.

   GuardDuty bewahrt Ihre Datei nicht länger als 30 Tage auf. Die Mitglieder des GuardDuty-Teams werden Ihre Einreichung analysieren und geeignete Maßnahmen ergreifen, um Ihre Erfahrung mit dem Malware Protection und dem GuardDuty-Service zu verbessern.

Behebung von Sicherheitsproblemen, die entdeckt wurden von GuardDuty

Amazon GuardDuty generiert Ergebnisse, die auf potenzielle Sicherheitsprobleme hinweisen. In dieser Version von GuardDuty deuten die potenziellen Sicherheitsprobleme entweder auf eine gefährdete EC2-Instance- oder Container-Workload oder auf eine Reihe kompromittierter Anmeldeinformationen in Ihrer Umgebung hin. AWS In den folgenden Abschnitten werden die empfohlenen Schritte zur Behebung für alle Szenarien beschrieben. Falls es alternative Behebungsszenarien gibt, werden diese im Eintrag für diesen spezifischen Erkenntnistyp beschrieben. Sie können auf die vollständigen Informationen zu einem Erkenntnistyp zugreifen, indem Sie ihn aus der Tabelle für aktive Erkenntnistypen auswählen.

Inhalt

Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance

Folgen Sie diesen empfohlenen Schritten, um eine potenziell gefährdete EC2-Instance in Ihrer Umgebung zu reparieren: AWS

1. Identifizieren Sie die potenziell gefährdete Amazon EC2 EC2-Instance

   Untersuchen Sie die potenziell kompromittierte Instance auf Malware und entfernen Sie sämtliche gefundene Malware. Sie können Malware-Scan auf Abruf verwenden, um Malware in der potenziell gefährdeten EC2-Instance zu identifizieren oder AWS Marketplace überprüfen, ob es hilfreiche Partnerprodukte zur Identifizierung und Entfernung von Malware gibt.

2. Isolieren Sie die potenziell gefährdete Amazon EC2 EC2-Instance

   Gehen Sie nach Möglichkeit wie folgt vor, um die potenziell gefährdete Instance zu isolieren:

   1. Erstellen Sie eine dedizierte Isolations-Sicherheitsgruppe.
   2. Erstellen Sie eine einzige Regel `0.0.0.0/0 (0-65535)` für den gesamten Datenverkehr in den ausgehenden Regeln.

      Wenn diese Regel gilt, wandelt sie den gesamten vorhandenen (und neuen) ausgehenden Verkehr in unbeaufsichtigten Datenverkehr um und blockiert alle bestehenden ausgehenden Sitzungen. Weitere Informationen finden Sie unter Verbindungen ohne Nachverfolgung.
   3. Entfernen Sie alle aktuellen Sicherheitsgruppenzuordnungen aus der potenziell gefährdeten Instanz.
   4. Ordnen Sie die Isolations-Sicherheitsgruppe dieser Instanz zu.

      Löschen Sie nach der Zuordnung die Regel `0.0.0.0/0 (0-65535)` für den gesamten Datenverkehr aus den ausgehenden Regeln der Isolations-Sicherheitsgruppe.
3. Identifizieren Sie die Quelle der verdächtigen Aktivität.

   Wenn Malware erkannt wird, identifizieren und beenden Sie anhand des Erkennungstyps in Ihrem Konto die potenziell nicht autorisierte Aktivität auf Ihrer EC2-Instance. Dies kann Aktionen wie das Schließen aller offenen Ports, das Ändern von Zugriffsrichtlinien und das Aktualisieren von Anwendungen zur Behebung von Schwachstellen erfordern.

   Wenn Sie nicht in der Lage sind, unbefugte Aktivitäten auf Ihrer potenziell gefährdeten EC2-Instance zu identifizieren und zu stoppen, empfehlen wir Ihnen, die gefährdete EC2-Instance zu beenden und sie bei Bedarf durch eine neue Instance zu ersetzen. Nachfolgend finden Sie weitere Ressourcen zum Schützen Ihrer EC2-Instances:

   - Abschnitte „Sicherheit und Netzwerk“ im Dokument Bewährte Methoden für Amazon EC2.
   - Amazon EC2-Sicherheitsgruppen für Linux-Instances und Amazon EC2-Sicherheitsgruppen für Windows-Instances.
   - Sicherheit in Amazon EC2
   - Tipps zum Sichern Ihrer EC2-Instances (Linux)
   - AWS Bewährte Sicherheitsmethoden
   - Vorfälle in der Infrastrukturdomäne am AWS
4. Durchsuchen AWS re:Post

AWS re:PostSuchen Sie nach weiterer Unterstützung.

5. Reichen Sie eine Anfrage für technischen Support ein

   Wenn Sie ein Premium-Support-Paket abonniert haben, können Sie eine Anfrage für den technischen Support senden.

Behebung eines potenziell gefährdeten S3-Buckets

Folgen Sie diesen empfohlenen Schritten, um einen potenziell gefährdeten Amazon S3 S3-Bucket in Ihrer AWS Umgebung zu beheben:

1. Identifizieren Sie die potenziell gefährdete S3-Ressource.

   Ein GuardDuty Ergebnis für S3 listet den zugehörigen S3-Bucket, seinen Amazon-Ressourcennamen (ARN) und seinen Besitzer in den Ergebnisdetails auf.

2. Identifizieren Sie die Quelle der verdächtigen Aktivität und des verwendeten API-Aufrufs.

   Der verwendete API-Aufruf wird in den Ergebnisdetails als `API` aufgelistet. Bei der Quelle handelt es sich um einen IAM-Prinzipal (entweder eine IAM-Rolle, ein IAM-Benutzer oder ein IAM-Konto) und identifizierende Details werden in der Erkenntnis aufgeführt. Je nach Quelltyp sind Informationen zur Remote-IP-Adresse oder zur Quelldomain verfügbar, anhand derer Sie beurteilen können, ob die Quelle autorisiert wurde. Wenn das Ergebnis Anmeldeinformationen von einer Amazon EC2 EC2-Instance betraf, werden die Details für diese Ressource ebenfalls aufgenommen.

3. Stellen Sie fest, ob die Anrufquelle autorisiert war, auf die identifizierte Ressource zuzugreifen.

   Denken Sie zum Beispiel an Folgendes:

   - Wenn ein IAM-Benutzer betroffen war, ist es möglich, dass seine Anmeldeinformationen möglicherweise kompromittiert wurden? Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.
   - Wenn eine API von einem Prinzipal aufgerufen wurde, der diesen API-Typ noch nie aufgerufen hat, benötigt diese Quelle dann Zugriffsberechtigungen für diesen Vorgang? Können die Bucket-Berechtigungen weiter eingeschränkt werden?
   - Wenn der Zugriff anhand des Benutzernamens `ANONYMOUS_PRINCIPAL` mit dem Benutzertyp `AWSAccount` erkannt wurde, bedeutet dies, dass der Bucket öffentlich ist und darauf zugegriffen wurde. Sollte dieser Bucket öffentlich sein? Falls nicht, finden Sie in den folgenden

Sicherheitsempfehlungen alternative Lösungen für die gemeinsame Nutzung von S3-Ressourcen.

- Wenn der Zugriff über einen erfolgreichen `PreflightRequest`-Aufruf erfolgte, wird anhand des Benutzernamens `ANONYMOUS_PRINCIPAL` mit dem Benutzertyp `AWSAccount` angezeigt, dass für den Bucket eine CORS-Richtlinie (Cross-Origin Resource Sharing) festgelegt wurde. Sollte dieser Bucket eine CORS-Richtlinie haben? Falls nicht, stellen Sie sicher, dass der Bucket nicht versehentlich öffentlich ist, und finden Sie in den folgenden Sicherheitsempfehlungen alternative Lösungen für die gemeinsame Nutzung von S3-Ressourcen. Weitere Informationen zu CORS und Amazon S3 finden Sie unter Cross-Origin Resource Sharing (CORS) verwenden im Benutzerhandbuch zu S3.

4. Stellen Sie fest, ob der S3-Bucket sensible Daten enthält.

   Verwenden Sie Amazon Macie, um zu ermitteln, ob der S3-Bucket sensible Daten, wie persönlich identifizierbare Informationen (PII), Finanzdaten oder Anmeldeinformationen enthält. Wenn die automatische Erkennung sensibler Daten für Ihr Macie-Konto aktiviert ist, überprüfen Sie die Details des S3-Buckets, um den Inhalt Ihres S3-Buckets besser zu verstehen. Wenn dieses Feature für Ihr Macie-Konto deaktiviert ist, empfehlen wir, es zu aktivieren, um Ihre Bewertung zu beschleunigen. Alternativ können Sie einen Discovery-Job für sensible Daten erstellen und ausführen, um die Objekte des S3-Buckets auf sensible Daten zu untersuchen. Weitere Informationen finden Sie unter Aufspüren sensibler Daten mit Macie.

Wenn der Zugriff autorisiert wurde, können Sie die Erkenntnis ignorieren. In der https://console.aws.amazon.com/guardduty/-Konsole können Sie Regeln einrichten, um einzelne Erkenntnisse vollständig zu unterdrücken, sodass sie nicht mehr angezeigt werden. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Wenn Sie feststellen, dass Ihre S3-Daten offengelegt wurden oder von Unbefugten darauf zugegriffen wurde, lesen Sie sich die folgenden S3-Sicherheitsempfehlungen durch, um die Zugriffsrechte zu verschärfen und den Zugriff einzuschränken. Welche Lösungen für die Behebung geeignet sind, hängt von den Anforderungen Ihrer spezifischen Umgebung ab.

Empfehlungen, die auf spezifischen Zugriffsanforderungen für S3-Buckets basieren

Die folgende Liste enthält Empfehlungen, die auf spezifischen Zugriffsanforderungen für Amazon S3 S3-Buckets basieren:

- Um den öffentlichen Zugriff auf Ihre S3-Datennutzung zentral einzuschränken, blockiert S3 den öffentlichen Zugriff. Die Einstellungen zum Blockieren des öffentlichen Zugriffs können für Access Points, Buckets und AWS Konten über vier verschiedene Einstellungen aktiviert werden, um die Granularität des Zugriffs zu steuern. Weitere Informationen finden Sie unter Einstellungen von S3 Block Public Access.
- AWS Mithilfe von Zugriffsrichtlinien können Sie steuern, wie IAM-Benutzer auf Ihre Ressourcen oder auf Ihre Buckets zugreifen können. Weitere Informationen dazu finden Sie unter Verwendung von Bucket-Richtlinien und Benutzerrichtlinien.

  Darüber hinaus können Sie Virtual Private Cloud (VPC)-Endpunkte mit S3-Bucket-Richtlinien verwenden, um den Zugriff auf bestimmte VPC-Endpunkte zu beschränken. Weitere Informationen finden Sie unter Beispiel-Bucket-Richtlinien für VPC-Endpunkte für Amazon S3.
- Um vertrauenswürdigen Entitäten außerhalb Ihres Kontos vorübergehend den Zugriff auf Ihre S3-Objekte zu gewähren, können Sie über S3 eine vorsignierte URL erstellen. Dieser Zugriff wird mit Ihren Konto-Anmeldeinformationen erstellt und kann je nach den verwendeten Anmeldeinformationen 6 Stunden bis 7 Tage dauern. Weitere Informationen finden Sie unter Generieren vorsignierter URLs mit S3.
- Für Anwendungsfälle, die die gemeinsame Nutzung von S3-Objekten zwischen verschiedenen Quellen erfordern, können Sie S3-Zugangspunkte verwenden, um Berechtigungssätze zu erstellen, die den Zugriff nur auf diejenigen innerhalb Ihres privaten Netzwerks beschränken. Weitere Informationen finden Sie unter Verwalten des Datenzugriffs mit Amazon S3 Access Points.
- Um anderen AWS Konten sicheren Zugriff auf Ihre S3-Ressourcen zu gewähren, können Sie eine Zugriffskontrollliste (ACL) verwenden. Weitere Informationen finden Sie unter S3-Zugriff mit ACLs verwalten.

Weitere Informationen zu den S3-Sicherheitsoptionen finden Sie unter Bewährte Methoden für S3 Security.

Behebung eines potenziell gefährdeten ECS-Clusters

Folgen Sie diesen empfohlenen Schritten, um einen potenziell gefährdeten Amazon ECS-Cluster in Ihrer AWS Umgebung zu beheben:

1. Identifizieren Sie den potenziell gefährdeten ECS-Cluster.

   Das GuardDuty Malware-Schutz-Ergebnis für ECS enthält die Details des ECS-Clusters im Detailbereich des Ergebnisses.

2. Bewerten Sie die Quelle der Malware

   Prüfen Sie, ob sich die entdeckte Malware im Image des Containers befand. Wenn das Image Schadsoftware enthielt, identifizieren Sie alle anderen Aufgaben, die mit diesem Image ausgeführt werden. Hinweise zur Ausführung von Aufgaben finden Sie unter ListTasks.

3. Isolieren Sie die potenziell betroffenen Aufgaben

   Isolieren Sie die betroffenen Aufgaben, indem Sie den gesamten ein- und ausgehenden Datenverkehr zu der Aufgabe verweigern. Eine Regel zum Ablehnen jeglichen Datenverkehrs kann Ihnen dabei helfen, einen Angriff zu stoppen, der bereits im Gange ist, indem alle Verbindungen zu der Aufgabe unterbrochen werden.

Wenn der Zugriff autorisiert wurde, können Sie die Erkenntnis ignorieren. In der https://console.aws.amazon.com/guardduty/-Konsole können Sie Regeln einrichten, um einzelne Erkenntnisse vollständig zu unterdrücken, sodass sie nicht mehr angezeigt werden. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Behebung potenziell gefährdeter Anmeldeinformationen AWS

Folgen Sie diesen empfohlenen Schritten, um potenziell kompromittierte Anmeldeinformationen in Ihrer Umgebung zu beheben: AWS

1. Identifizieren Sie die potenziell gefährdete IAM-Entität und den verwendeten API-Aufruf.

   Der verwendete API-Aufruf wird in den Ergebnisdetails als `API` aufgelistet. Die IAM-Entität (entweder eine IAM-Rolle oder ein IAM-Benutzer) und ihre identifizierenden Informationen werden im Abschnitt „Ressourcen“ der Ergebnisdetails aufgeführt. Der Typ der beteiligten IAM-Entität kann anhand des Feldes Benutzertyp bestimmt werden. Der Name der IAM-Entität befindet sich im Feld Benutzername. Der Typ von IAM-Entität, der an einem Ergebnis beteiligt ist, kann auch anhand der verwendeten Zugriffsschlüssel-ID bestimmt werden.

   Für Schlüssel, die mit `AKIA` beginnen:

   Bei dieser Art von Schlüssel handelt es sich um langfristige, vom Kunden verwaltete Anmeldeinformationen, die einem IAM-Benutzer oder Root-Benutzer des AWS-Kontos zugeordnet sind. Weitere Informationen zum Verwalten von Zugriffsschlüsseln für IAM-Benutzer finden Sie unter Verwalten von Zugriffsschlüsseln für IAM-Benutzer.

Für Schlüssel, die mit `ASIA` beginnen:

Bei dieser Art von Schlüssel handelt es sich um kurzfristige temporäre Anmeldeinformationen, die von AWS Security Token Service generiert werden. Diese Schlüssel existieren nur für kurze Zeit und können in der AWS Management Console nicht angezeigt oder verwaltet werden. IAM-Rollen verwenden immer AWS STS Anmeldeinformationen, sie können aber auch für IAM-Benutzer generiert werden. Weitere Informationen AWS STS finden Sie unter IAM: Temporäre Sicherheitsanmeldeinformationen.

Wenn eine Rolle verwendet wurde, enthält das Feld Benutzername den Namen der verwendeten Rolle. Sie können feststellen, wie der Schlüssel angefordert wurde, AWS CloudTrail indem Sie das `sessionIssuer` Element des CloudTrail Protokolleintrags untersuchen. Weitere Informationen finden Sie unter IAM und Informationen unter. AWS STS CloudTrail

2. Überprüfen Sie die Berechtigungen für die IAM-Entität.

   Öffnen Sie die IAM-Konsole. Wählen Sie je nach Typ der verwendeten Entität die Registerkarte Benutzer oder Rollen und suchen Sie nach der betroffenen Entität, indem Sie den identifizierten Namen in das Suchfeld eingeben. Überprüfen Sie über die Registerkarten Berechtigung und Access Advisor effektive Berechtigungen für diese Entität.

3. Bestimmen Sie, ob die Anmeldeinformationen der IAM-Entität rechtmäßig verwendet wurden.

   Wenden Sie sich an den Benutzer der Anmeldeinformationen, um festzustellen, ob die Aktivität beabsichtigt war.

   Ermitteln Sie beispielsweise, ob der Benutzer die Anmeldeinformationen zu Folgendem verwendet hat:

   - Hat den API-Vorgang aufgerufen, der im GuardDuty Ergebnis aufgeführt war
   - Der API-Vorgang wurde zu dem Zeitpunkt aufgerufen, der im Ergebnis aufgeführt ist GuardDuty
   - Der API-Vorgang wurde von der IP-Adresse aus aufgerufen, die im Ergebnis aufgeführt ist GuardDuty

Wenn es sich bei dieser Aktivität um eine legitime Verwendung der AWS Anmeldeinformationen handelt, können Sie den GuardDuty Befund ignorieren. In der https://console.aws.amazon.com/guardduty/-Konsole können Sie Regeln einrichten, um einzelne Erkenntnisse vollständig zu unterdrücken, sodass sie nicht mehr angezeigt werden. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Wenn Sie nicht bestätigen können, ob es sich bei dieser Aktivität um eine legitime Verwendung handelt, könnte dies das Ergebnis einer Kompromittierung des jeweiligen Zugriffsschlüssels sein — der Anmeldedaten des IAM-Benutzers oder möglicherweise der gesamten. AWS-Konto Wenn Sie vermuten, dass Ihre Anmeldeinformationen kompromittiert wurden, lesen Sie die Informationen im Artikel Meine Daten sind AWS-Konto möglicherweise kompromittiert, um dieses Problem zu beheben.

Behebung eines potenziell gefährdeten Standalone-Containers

1. Isolieren Sie den potenziell gefährdeten Container

   Mithilfe der folgenden Schritte können Sie den potenziell schädlichen Container-Workload identifizieren:

   - Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
   - Wählen Sie auf der Ergebnisseite das entsprechende Ergebnis aus, um das Ergebnisfenster aufzurufen.
   - Im Erkenntnisfenster können Sie im Abschnitt Betroffene Ressource die ID und den Namen des Containers einsehen.

   Isolieren Sie diesen Container von anderen Container-Workloads.
2. Halten Sie den Container an

   Unterbrechen Sie alle Prozesse in Ihrem Container.

   Informationen zum Einfrieren Ihres Containers finden Sie unter Einen Container pausieren.

   Stoppen Sie den Container

   Wenn der obige Schritt fehlschlägt und der Container nicht angehalten wird, beenden Sie die Ausführung des Containers. Wenn Sie die Snapshot-Beibehaltung Funktion aktiviert haben, GuardDuty werden die Snapshots Ihrer EBS-Volumes, die Malware enthalten, beibehalten.

   Informationen zum Stoppen des Containers finden Sie unter Stoppen eines Containers.
3. Prüfen Sie das Vorhandensein von Malware

   Prüfen Sie, ob sich die entdeckte Malware im Image des Containers befand.

Wenn der Zugriff autorisiert wurde, können Sie die Erkenntnis ignorieren. In der https://console.aws.amazon.com/guardduty/-Konsole können Sie Regeln einrichten, um einzelne

Erkenntnisse vollständig zu unterdrücken, sodass sie nicht mehr angezeigt werden. In der GuardDuty Konsole können Sie Regeln einrichten, um einzelne Ergebnisse vollständig zu unterdrücken, sodass sie nicht mehr angezeigt werden. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Behebung der Erkenntnisse von EKS Audit Log Monitoring

Amazon GuardDuty generiert Ergebnisse, die auf potenzielle Kubernetes-Sicherheitsprobleme hinweisen, wenn EKS Audit Log Monitoring für Ihr Konto aktiviert ist. Weitere Informationen finden Sie unter EKS Audit Log Monitoring. In den folgenden Abschnitten werden die empfohlenen Schritte zur Behebung für alle Szenarien beschrieben. Spezifische Behebungsmaßnahmen werden im Eintrag für diesen spezifischen Erkenntnistyp beschrieben. Sie können auf die vollständigen Informationen zu einem Erkenntnistyp zugreifen, indem Sie ihn aus der Tabelle für aktive Erkenntnistypen auswählen.

Wenn einer der Erkennungstypen von EKS Audit Log Monitoring erwartungsgemäß generiert wurde, können Sie erwägen, Unterdrückungsregeln hinzuzufügen, um zukünftige Warnmeldungen zu verhindern.

Verschiedene Arten von Angriffen und Konfigurationsproblemen können GuardDuty Kubernetes-Erkenntnisse auslösen. Dieser Leitfaden hilft Ihnen dabei, die Ursachen für GuardDuty Erkenntnisse in Ihrem Cluster zu identifizieren und geeignete Anleitungen zur Behebung zu finden. Im Folgenden sind die Hauptursachen aufgeführt, die zu GuardDuty Kubernetes-Ergebnissen führen:

- Mögliche Konfigurationsprobleme
- Behebung potenziell kompromittierter Kubernetes-Benutzer
- Behebung potenziell kompromittierter Kubernetes-Pods
- Behebung potenziell kompromittierter Kubernetes-Knoten
- Behebung potenziell kompromittierter Container-Images

> **Note**
>
> Vor Kubernetes Version 1.14 war die `system:unauthenticated` Gruppe `system:basic-user` ClusterRoles standardmäßig `system:discovery` und zugeordnet. Dies könnte unbeabsichtigten Zugriff durch anonyme Benutzer ermöglichen. Durch Cluster-Updates werden diese Berechtigungen nicht aufgehoben. Das bedeutet, dass diese Berechtigungen auch dann noch gültig sind, wenn Sie Ihren Cluster auf Version 1.14 oder höher aktualisiert haben. Wir empfehlen, dass Sie die Zuordnung dieser Berechtigungen zu der `system:unauthenticated`-Gruppe aufheben.

Weitere Informationen zum Entfernen dieser Berechtigungen finden Sie unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch.

Mögliche Konfigurationsprobleme

Wenn eine Erkenntnis auf ein Konfigurationsproblem hindeutet, finden Sie im Abschnitt zur Behebung dieses Fehlers Anleitungen zur Lösung dieses speziellen Problems. Weitere Informationen finden Sie unter den folgenden Erkenntnistypen, die auf Konfigurationsprobleme hinweisen:

- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/KubeflowDashboardExposed
- Jede Erkenntnis, die auf endet SuccessfulAnonymousAccess

Behebung potenziell kompromittierter Kubernetes-Benutzer

Eine GuardDuty Erkenntnis kann auf einen kompromittierten Kubernetes-Benutzer hinweisen, wenn ein in der Erkenntnis identifizierter Benutzer eine unerwartete API-Aktion ausgeführt hat. Sie können den Benutzer im Bereich Kubernetes-Benutzerdetails im Erkenntnisfenster der Konsole oder in der `resources.eksClusterDetails.kubernetesDetails.kubernetesUserDetails` der JSON-Datei mit den Erkenntnissen identifizieren. Zu diesen Benutzerdetails gehören `user name`, `uid` und die Kubernetes-Gruppen, zu denen der Benutzer gehört.

Wenn der Benutzer mit einer IAM-Entität auf den Workload zugegriffen hat, können Sie den `Access Key details`-Abschnitt verwenden, um die Details einer IAM-Rolle oder eines IAM-Benutzers zu identifizieren. Sehen Sie sich die folgenden Benutzertypen und deren Anleitungen zur Problembehebung an.

> **Note**
>
> Sie können Amazon Detective verwenden, um die in der Erkenntnis identifizierte IAM-Rolle oder den IAM-Benutzer genauer zu untersuchen. Wählen Sie beim Anzeigen der Erkenntnisdetails in der GuardDuty Konsole Untersuchen in Detective aus. Wählen Sie dann

AWS Benutzer oder Rolle aus den aufgelisteten Elementen aus, um sie in Detective zu untersuchen.

Integrierter Kubernetes-Admin – Der Standardbenutzer, der von Amazon EKS der IAM-Identität zugewiesen wurde, die den Cluster erstellt hat. Dieser Benutzertyp wird durch den Benutzernamen identifiziert `kubernetes-admin`.

Wie Sie einem integrierten Kubernetes-Administrator den Zugriff entziehen:

- Identifizieren Sie den `userType` aus dem `Access Key details`-Abschnitt.
  - Wenn der `userType` Rolle ist und die Rolle zu einer EC2-Instance-Rolle gehört:
    - Identifizieren Sie diese Instance und folgen Sie dann den Anweisungen unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.
  - Wenn es sich bei `userType` um einen Benutzer handelt oder um eine Rolle, die von einem Benutzer übernommen wurde:
    1. Rotieren Sie den Zugriffsschlüssel dieses Benutzers.
    2. Rotieren Sie alle Geheimnisse, auf die der Benutzer Zugriff hatte.
    3. Weitere Informationen finden Sie unter Mein AWS Konto ist möglicherweise kompromittiert.

OIDC-authentifizierter Benutzer – Ein Benutzer, dem der Zugriff über einen OIDC-Anbieter gewährt wurde. In der Regel hat ein OIDC-Benutzer eine E-Mail-Adresse als Benutzernamen. Sie können mit den folgenden Befehl überprüfen, ob Ihr Cluster OIDC verwendet: `aws eks list-identity-provider-configs --cluster-name` *`your-cluster-name`*

Um einem OIDC-authentifizierten Benutzer den Zugriff zu entziehen:

1. Rotieren Sie die Anmeldeinformationen dieses Benutzers im OIDC-Anbieter.
2. Rotieren Sie alle Geheimnisse, auf die der Benutzer Zugriff hatte.

AWS-Auth ConfigMap -definierter Benutzer – Ein IAM-Benutzer, dem über eine AWS-Auth Zugriff gewährt wurde ConfigMap. Weitere Informationen finden Sie unter Verwalten von Benutzern oder IAM-Rollen für Ihren Cluster im EKS-Benutzerhandbuch. Sie können ihre Berechtigungen überprüfen, indem Sie den folgenden Befehl verwenden: `kubectl edit configmaps aws-auth --namespace kube-system`

So widerrufen Sie den Zugriff eines AWS ConfigMap-Benutzers:

1. Verwenden Sie den folgenden Befehl, um die zu öffnen ConfigMap.

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. Identifizieren Sie den Rollen- oder Benutzereintrag im Abschnitt mapRoles oder mapUsers mit demselben Benutzernamen wie dem im Abschnitt Kubernetes-Benutzerdetails Ihrer GuardDuty Erkenntnis gemeldeten. Sehen Sie sich das folgende Beispiel an, in dem der Admin-Benutzer in einer Erkenntnis identifiziert wurde.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      user name: system:node:EC2_PrivateDNSName
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::123456789012:user/admin
      username: admin
      groups:
        - system:masters
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

3. Entfernen Sie diesen Benutzer aus der ConfigMap. Sehen Sie sich das folgende Beispiel an, in dem der Admin-Benutzer entfernt wurde.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::111122223333:user/ops-user
```

```
    username: ops-user
    groups:
      - system:masters
```

4. Wenn es sich bei `userType` um einen Benutzer handelt oder um eine Rolle, die von einem Benutzer übernommen wurde:
   a. Rotieren Sie den Zugriffsschlüssel dieses Benutzers.
   b. Rotieren Sie alle Geheimnisse, auf die der Benutzer Zugriff hatte.
   c. Weitere Informationen finden Sie unter Mein AWS Konto ist möglicherweise kompromittiert.

Wenn die Erkenntnis keinen `resource.accessKeyDetails`-Abschnitt enthält, handelt es sich bei dem Benutzer um ein Kubernetes-Servicekonto.

Servicekonto – Das Servicekonto stellt eine Identität für Pods bereit und kann anhand eines Benutzernamens mit dem folgenden Format identifiziert werden: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Um den Zugriff auf ein Servicekonto zu widerrufen:

1. Rotieren Sie die Anmeldeinformationen für das Servicekonto.
2. Lesen Sie die Hinweise zur Pod-Kompromittierung im folgenden Abschnitt.

Behebung potenziell kompromittierter Kubernetes-Pods

Wenn Details zu einer Pod- oder Workload-Ressource innerhalb des `resource.kubernetesDetails.kubernetesWorkloadDetails` Abschnitts GuardDuty angibt, wurde diese Pod- oder Workload-Ressource möglicherweise kompromittiert. Eine GuardDuty Erkenntnis kann darauf hinweisen, dass ein einzelner Pod kompromittiert wurde oder dass mehrere Pods über eine übergeordnete Ressource kompromittiert wurden. In den folgenden Kompromissszenarien finden Sie Anleitungen zur Identifizierung des oder der Pods, die kompromittiert wurden.

Kompromittierung einzelner Pods

Wenn es sich bei dem `type`-Feld innerhalb des `resource.kubernetesDetails.kubernetesWorkloadDetails`-Abschnitts um Pods handelt, identifiziert die Erkenntnis einzelne Pods. Das Namensfeld ist der `name` der Pods und das `namespace`-Feld ist sein Namespace.

Informationen zum Identifizieren des Worker-Knotens, auf dem die Pods ausgeführt werden, finden Sie unter Identifizieren der angegriffenen Pods und Worker-Knoten.

Pods wurden über die Workload-Ressource kompromittiert

Wenn das `type`-Feld innerhalb des `resource.kubernetesDetails.kubernetesWorkloadDetails`-Abschnitts eine Workload-Ressource identifiziert, z. B. eine `Deployment`, ist es wahrscheinlich, dass alle Pods innerhalb dieser Workload-Ressource kompromittiert wurden.

Informationen zum Identifizieren aller Pods der Workload-Ressource und der Knoten, auf denen sie ausgeführt werden, finden Sie unter Identifizieren der angegriffenen Pods und Worker-Knoten mithilfe des Workload-Namens .

Pods wurden über das Servicekonto kompromittiert

Wenn eine GuardDuty Erkenntnis ein Servicekonto im `resource.kubernetesDetails.kubernetesUserDetails` Abschnitt identifiziert, ist es wahrscheinlich, dass Pods, die das identifizierte Servicekonto verwenden, kompromittiert werden. Der durch eine Erkenntnis gemeldete Benutzername ist ein Servicekonto, wenn er das folgende Format hat: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Informationen zum Identifizieren aller Pods mithilfe des Servicekontos und der Knoten, auf denen sie ausgeführt werden, finden Sie unter Identifizieren der fehlerhaften Pods und Worker-Knoten mithilfe des Servicekontonamens .

Nachdem Sie alle kompromittierten Pods und die Knoten identifiziert haben, auf denen sie ausgeführt werden, lesen Sie den Leitfaden für bewährte Methoden von Amazon EKS, um den Pod zu isolieren, seine Anmeldeinformationen zu rotieren und Daten für forensische Analysen zu sammeln.

So beheben Sie einen potenziell kompromittierten Pod:

1. Identifizieren Sie die Schwachstelle, durch die die Pods gefährdet wurden.
2. Implementieren Sie das Update für diese Schwachstelle und starten Sie neue Ersatz-Pods.
3. Löschen Sie die anfälligen Pods.

   Weitere Informationen finden Sie unter Kompromittierte Pod- oder Workload-Ressource erneut bereitstellen.

Wenn dem Worker-Knoten eine IAM-Rolle zugewiesen wurde, die es Pods ermöglicht, Zugriff auf andere AWS Ressourcen zu erhalten, entfernen Sie diese Rollen aus der Instance, um weitere Beschädigungen durch den Angriff zu verhindern. Wenn dem Pod eine IAM-Rolle zugewiesen wurde, sollten Sie ebenfalls prüfen, ob Sie die IAM-Richtlinien sicher aus der Rolle entfernen können, ohne andere Workloads zu beeinträchtigen.

Behebung potenziell kompromittierter Container-Images

Wenn eine GuardDuty Erkenntnis auf eine Pod-Kompromittierung hinweist, kann das zum Starten des Pods verwendete Image potenziell bösartig oder kompromittiert sein. GuardDuty Erkenntnis identifizieren das Container-Image im `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` Feld . Sie können feststellen, ob das Image bösartig ist, indem Sie es auf Malware scannen.

So beheben Sie ein potenziell kompromittiertes Container-Image:

1. Beenden Sie sofort die Verwendung des Images und entfernen Sie es aus Ihrem Image-Repository.
2. Identifizieren Sie alle Pods, die das potenziell kompromittierte Image verwenden.

   Weitere Informationen finden Sie unter Identifizieren von Pods mit potenziell anfälligen oder kompromittierten Container-Images und Worker-Knoten.
3. Isolieren Sie die potenziell gefährdeten Pods, rotieren Sie die Anmeldeinformationen und sammeln Sie Daten für die Analyse. Weitere Informationen finden Sie im Leitfaden zu bewährten Methoden für Amazon EKS.
4. Löschen Sie alle Pods mit dem potenziell kompromittierten Image.

Behebung potenziell kompromittierter Kubernetes-Knoten

Eine GuardDuty Erkenntnis kann auf eine Knotenkompromittierung hinweisen, wenn der in der Erkenntnis identifizierte Benutzer eine Knotenidentität darstellt oder wenn die Erkenntnis die Verwendung eines privilegierten Containers anzeigt.

Die Benutzeridentität ist ein Worker-Knoten, wenn das Feld für den Benutzernamen das folgende Format hat: `system:node:node name`. Beispiel: `system:node:ip-192-168-3-201.ec2.internal` Dies weist darauf hin, dass der Angreifer Zugriff auf den Knoten erhalten hat und die Anmeldeinformationen des Knotens verwendet, um mit dem Kubernetes-API-Endpunkt zu kommunizieren.

Eine Erkenntnis weist auf die Verwendung eines privilegierten Containers hin, wenn für einen oder mehrere der in der Erkenntnis aufgelisteten Container das Erkenntnisfeld `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.` auf `True` gesetzt ist.

So beheben Sie einen potenziell kompromittierten Knoten:

1. Isolieren Sie den Pod, rotieren Sie seine Anmeldeinformationen und sammeln Sie Daten für die forensische Analyse.

   Weitere Informationen finden Sie im Leitfaden zu bewährten Methoden für Amazon EKS.
2. Identifizieren Sie die Servicekonten, die von allen Pods verwendet werden, die auf dem potenziell kompromittierten Knoten ausgeführt werden. Überprüfen Sie ihre Berechtigungen und rotieren Sie die Servicekonten bei Bedarf.
3. Beenden Sie den potenziell kompromittierten Knoten.

Behebung der Ergebnisse von Runtime Monitoring

Wenn Sie Runtime Monitoring für Ihr Konto aktivieren, generiert Amazon GuardDuty möglicherweise InformationenRuntime Monitoring: Typen finden, die auf potenzielle Sicherheitsprobleme in Ihrer AWS Umgebung hinweisen. Die potenziellen Sicherheitsprobleme deuten entweder auf eine kompromittierte Amazon EC2 EC2-Instance, einen Container-Workload, einen Amazon EKS-Cluster oder eine Reihe kompromittierter Anmeldeinformationen in Ihrer Umgebung hin. AWS Der Security Agent überwacht Runtime-Ereignisse von mehreren Ressourcentypen aus. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie sich den Ressourcentyp in den generierten Suchdetails in der GuardDuty Konsole an. Im folgenden Abschnitt werden die empfohlenen Behebungsschritte für alle Szenarien beschrieben.

Instance

Wenn der Ressourcentyp in den Erkenntnisdetails Instance lautet, deutet dies darauf hin, dass entweder eine EC2-Instance oder ein EKS-Knoten potenziell kompromittiert ist.

- Informationen zur Behebung eines kompromittierten EKS-Knotens finden Sie unter Behebung potenziell kompromittierter Kubernetes-Knoten.
- Informationen zur Behebung einer kompromittierten EC2-Instance finden Sie unter Behebung einer potenziell gefährdeten Amazon EC2 EC2-Instance.

EKSCluster

Wenn der Ressourcentyp in den Erkenntnisdetails EKSCluster lautet, deutet dies darauf hin, dass entweder ein Pod oder ein Container in einem EKS-Cluster potenziell kompromittiert ist.

- Informationen zur Behebung eines kompromittierten Pods finden Sie unter Behebung potenziell kompromittierter Kubernetes-Pods.
- Informationen zur Behebung eines kompromittierten Container-Images finden Sie unter Behebung potenziell kompromittierter Container-Images.

ECSCluster

Wenn der Ressourcentyp in den Ergebnisdetails ecsCluster lautet, bedeutet dies, dass entweder eine ECS-Task oder ein Container innerhalb einer ECS-Task potenziell gefährdet ist.

1. Identifizieren Sie den betroffenen ECS-Cluster

   Das GuardDuty Runtime Monitoring-Ergebnis enthält die ECS-Cluster-Details im Detailbereich des Ergebnisses oder im `resource.ecsClusterDetails` Abschnitt in der Ergebnis-JSON.

2. Identifizieren Sie die betroffene ECS-Aufgabe

   Das GuardDuty Runtime Monitoring-Ergebnis enthält die ECS-Aufgabendetails im Detailbereich des Ergebnisses oder im `resource.ecsClusterDetails.taskDetails` Abschnitt in der Ergebnis-JSON.

3. Isolieren Sie die betroffene Aufgabe

   Isolieren Sie die betroffene Aufgabe, indem Sie den gesamten eingehenden und ausgehenden Datenverkehr für die Aufgabe verweigern. Eine Regel zum Verweigern des gesamten Datenverkehrs kann dazu beitragen, einen Angriff zu stoppen, der bereits im Gange ist, indem alle Verbindungen zu der Aufgabe unterbrochen werden.

4. Korrigieren Sie die gefährdete Aufgabe

   a. Identifizieren Sie die Sicherheitsanfälligkeit, die die Aufgabe gefährdet hat.

   b. Implementieren Sie das Update für diese Sicherheitsanfälligkeit und starten Sie eine neue Ersatzaufgabe.

   c. Beenden Sie die anfällige Aufgabe.

Container

Wenn der Ressourcentyp in den Erkenntnisdetails Container lautet, deutet dies darauf hin, dass ein alleinstehender Container potenziell kompromittiert ist.

- Informationen zur Problembehebung finden Sie unter Behebung eines potenziell gefährdeten Standalone-Containers.
- Falls die Erkenntnis für mehrere Container mit demselben Container-Image generiert wird, finden Sie weitere Informationen unter Behebung potenziell kompromittierter Container-Images.
- Wenn der Container auf den zugrunde liegenden EC2-Host zugegriffen hat, wurden die zugehörigen Instance-Anmeldeinformationen möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung potenziell gefährdeter Anmeldeinformationen AWS.
- Wenn ein potenziell böswilliger Akteur auf den zugrunde liegenden EKS-Knoten oder eine EC2-Instance zugegriffen hat, finden Sie unter den Registerkarten EKSCluster und Instance die empfohlenen Abhilfemaßnahmen.

Behebung kompromittierter Container-Images

Wenn ein GuardDuty Ergebnis darauf hindeutet, dass die Aufgabe kompromittiert wurde, könnte das zum Starten der Aufgabe verwendete Image bösartig oder beschädigt sein. GuardDuty Die Ergebnisse identifizieren das Container-Image innerhalb des `resource.ecsClusterDetails.taskDetails.containers.image` Felds. Sie können feststellen, ob das Bild bösartig ist, indem Sie es auf Malware scannen.

Um ein kompromittiertes Container-Image zu korrigieren

1. Beenden Sie sofort die Verwendung des Images und entfernen Sie es aus Ihrem Image-Repository.
2. Identifizieren Sie alle Aufgaben, die dieses Image verwenden.
3. Beenden Sie alle Aufgaben, die das kompromittierte Image verwenden. Aktualisieren Sie ihre Aufgabendefinitionen, sodass sie das kompromittierte Image nicht mehr verwenden.

Behebung einer potenziell kompromittierten Datenbank

GuardDuty generiert Erkenntnistypen für RDS Protection, die auf potenziell verdächtiges und anomales Anmeldeverhalten in Ihrem hinweisen, Unterstützte Datenbanken nachdem Sie aktiviert

habenGuardDuty RDS-Schutz. Mithilfe der RDS-Anmeldeaktivität GuardDuty analysiert und profiliert Bedrohungen, indem ungewöhnliche Muster bei Anmeldeversuchen identifiziert werden.

> **Note**
>
> Sie können auf die vollständigen Informationen zu einem Erkenntnistyp zugreifen, indem Sie ihn aus der Tabelle mit den Erkenntnissen auswählen.

Befolgen Sie diese empfohlenen Schritte, um eine potenziell kompromittierte Amazon-Aurora-Datenbank in Ihrer AWS Umgebung zu beheben.

Themen

- Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen
- Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen
- Behebung potenziell kompromittierter Anmeldeinformationen
- Einschränken von Netzwerkzugriff

Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen

Die folgenden empfohlenen Schritte können Ihnen helfen, eine potenziell gefährdete Aurora-Datenbank zu beheben, die im Zusammenhang mit erfolgreichen Anmeldeereignissen ungewöhnliches Verhalten zeigt.

1. Identifizieren Sie die betroffene Datenbank und den betroffenen Benutzer.

   Die generierte GuardDuty Erkenntnis enthält den Namen der betroffenen Datenbank und die entsprechenden Benutzerdetails. Weitere Informationen finden Sie unter Erkenntnisdetails.

2. Bestätigen Sie, ob dieses Verhalten erwartet oder unerwartet ist.

   In der folgenden Liste sind mögliche Szenarien aufgeführt, die dazu geführt GuardDuty haben könnten, dass ein Ergebnis generiert hat:

   - Ein Benutzer, der sich nach Ablauf einer langen Zeit bei seiner Datenbank anmeldet.
   - Ein Benutzer, der sich gelegentlich bei seiner Datenbank anmeldet, z. B. ein Finanzanalyst, der sich vierteljährlich anmeldet.

- Ein potenziell verdächtiger Akteur, der an einem erfolgreichen Anmeldeversuch beteiligt ist, gefährdet möglicherweise die Datenbank.

3. Beginnen Sie mit diesem Schritt, wenn das Verhalten unerwartet ist.

   1. Beschränken Sie den Datenbankzugriff

      Beschränken Sie den Datenbankzugriff für die verdächtigen Konten und die Quelle dieser Anmeldeaktivität. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Anmeldeinformationen und Einschränken von Netzwerkzugriff.

   2. Beurteilen Sie die Auswirkungen und stellen Sie fest, auf welche Informationen zugegriffen wurde.

      - Falls verfügbar, überprüfen Sie die Prüfungsprotokolle, um festzustellen, auf welche Informationen möglicherweise zugegriffen wurde. Weitere Informationen finden Sie unter Überwachung von Ereignissen, Protokollen und Streams in einem Amazon-Aurora-DB-Cluster im Amazon-Aurora-Benutzerhandbuch.
      - Stellen Sie fest, ob auf vertrauliche oder geschützte Informationen zugegriffen oder diese geändert wurden.

Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen

Die folgenden empfohlenen Schritte können Ihnen helfen, eine potenziell gefährdete Aurora-Datenbank zu beheben, die im Zusammenhang mit erfolglosen Anmeldeereignissen ungewöhnliches Verhalten zeigt.

1. Identifizieren Sie die betroffene Datenbank und den betroffenen Benutzer.

   Die generierte GuardDuty Erkenntnis enthält den Namen der betroffenen Datenbank und die entsprechenden Benutzerdetails. Weitere Informationen finden Sie unter Erkenntnisdetails.

2. Identifizieren Sie die Quelle der fehlgeschlagenen Anmeldeversuche.

   Die generierte GuardDuty Erkenntnis stellt die IP-Adresse und die ASN-Organisation (falls es sich um eine öffentliche Verbindung handelte) im Abschnitt Akteur des Erkenntnisbereichs bereit.

   Ein Autonomes System (AS) ist eine Gruppe von einem oder mehreren IP-Präfixen (Listen von IP-Adressen, auf die in einem Netzwerk zugegriffen werden kann), die von einem oder mehreren Netzwerkbetreibern betrieben werden und eine einzige, klar definierte Routing-Richtlinie

einhalten. Netzbetreiber benötigen autonome Systemnummern (ASNs), um das Routing in ihren Netzwerken zu kontrollieren und Routing-Informationen mit anderen Internetdienstanbietern (ISPs) auszutauschen.

3. Bestätigen Sie, dass dieses Verhalten unerwartet ist.

   Prüfen Sie wie folgt, ob diese Aktivität einen Versuch darstellt, zusätzlichen unbefugten Zugriff auf die Datenbank zu erlangen:

   - Wenn es sich um eine interne Quelle handelt, überprüfen Sie, ob eine Anwendung falsch konfiguriert ist, und wiederholt versucht, eine Verbindung herzustellen.
   - Handelt es sich um einen externen Akteur, prüfen Sie, ob die entsprechende Datenbank öffentlich zugänglich ist oder ob sie falsch konfiguriert ist, sodass potenzielle böswillige Akteure gängige Benutzernamen mit Brute-Force-Angriffen verwenden können.

4. Beginnen Sie mit diesem Schritt, wenn das Verhalten unerwartet ist.

   1. Beschränken Sie den Datenbankzugriff

      Beschränken Sie den Datenbankzugriff für die verdächtigen Konten und die Quelle dieser Anmeldeaktivität. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Anmeldeinformationen und Einschränken von Netzwerkzugriff.

   2. Führen Sie eine Ursachenanalyse durch und ermitteln Sie die Schritte, die möglicherweise zu dieser Aktivität geführt haben.

      Richten Sie eine Warnung ein, um benachrichtigt zu werden, wenn eine Aktivität eine Netzwerkrichtlinie ändert und zu einem unsicheren Zustand führt. Weitere Informationen finden Sie unter Firewall-Richtlinien in AWS Network Firewall im Entwicklerhandbuch fürAWS Network Firewall .

Behebung potenziell kompromittierter Anmeldeinformationen

Eine GuardDuty Erkenntnis kann darauf hinweisen, dass die Benutzeranmeldeinformationen für eine betroffene Datenbank kompromittiert wurden, wenn der in der Erkenntnis identifizierte Benutzer einen unerwarteten Datenbankvorgang ausgeführt hat. Sie können den Benutzer im Bereich RDS-DB-Benutzerdetails im Suchfenster der Konsole oder in der `resource.rdsDbUserDetails` der JSON-Datei mit den Erkenntnissen identifizieren. Zu diesen Benutzerdetails gehören der Benutzername, die verwendete Anwendung, die abgerufene Datenbank, die SSL-Version und die Authentifizierungsmethode.

- Informationen zum Widerrufen des Zugriffs oder zum Wechseln von Passwörtern für bestimmte Benutzer, die an der Erkenntnis beteiligt sind, finden Sie unter Sicherheit mit Amazon Aurora MySQL oder Sicherheit mit Amazon Aurora PostgreSQL im Amazon-Aurora-Benutzerhandbuch.
- Verwenden Sie AWS Secrets Manager , um die Secrets für Amazon Relational Database Service (RDS)-Datenbanken sicher zu speichern und automatisch zu rotieren. Weitere Informationen finden Sie unter AWS Secrets Manager -Konzepte im AWS Secrets Manager -Benutzerhandbuch.
- Verwenden Sie die IAM-Datenbankauthentifizierung, um den Zugriff von Datenbankbenutzern zu verwalten, ohne dass Passwörter erforderlich sind. Weitere Informationen finden Sie unter IAM-Datenbank-Authentifizierung im Amazon Aurora-Benutzerhandbuch.

  Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon Relational Database Service im Amazon-RDS-Benutzerhandbuch.

Einschränken von Netzwerkzugriff

Eine GuardDuty Erkenntnis kann darauf hinweisen, dass über Ihre Anwendungen oder Virtual Private Cloud (VPC) hinaus auf eine Datenbank zugegriffen werden kann. Wenn es sich bei der Remote-IP-Adresse in der Erkenntnis um eine unerwartete Verbindungsquelle handelt, überprüfen Sie die Sicherheitsgruppen. Eine Liste der an die Datenbank angehängten Sicherheitsgruppen ist in der Konsole https://console.aws.amazon.com/rds/ unter Sicherheitsgruppen oder in der `resource.rdsDbInstanceDetails.dbSecurityGroups` JSON-Datei der Erkenntnisse verfügbar. Weitere Informationen zur Konfiguration von Sicherheitsgruppen finden Sie unter Zugriffskontrolle mit Sicherheitsgruppen im Amazon-RDS-Benutzerhandbuch.

Wenn Sie eine Firewall verwenden, schränken Sie den Netzwerkzugriff auf die Datenbank ein, indem Sie die Network Access Control Lists (NACLs) neu konfigurieren. Weitere Informationen finden Sie unter Firewall-Richtlinien in AWS Network Firewall im Entwicklerhandbuch fürAWS Network Firewall .

Behebung einer potenziell kompromittierten Lambda-Funktion

Wenn eine Lambda-Protection-Erkenntnis GuardDuty generiert und die Aktivität unerwartet ist, ist Ihre Lambda-Funktion möglicherweise kompromittiert. Wir empfehlen, die folgenden Schritte auszuführen, um eine kompromittierte Lambda-Funktion zu beheben.

So beheben Sie Erkenntnisse von Lambda Protection

1. Identifizieren Sie die potenziell kompromittierte Lambda-Funktionsversion .

Eine GuardDuty Erkenntnis für Lambda Protection enthält den Namen, den Amazon-Ressourcennamen (ARN), die Funktionsversion und die Revisions-ID, die der in den Erkenntnisdetails aufgeführten Lambda-Funktion zugeordnet sind.

2. Identifizieren Sie die Quelle der potenziell verdächtigen Aktivität .

   a. Überprüfen Sie den Code, der der Lambda-Funktionsversion zugeordnet ist, die an der Erkenntnis beteiligt war.

   b. Überprüfen Sie die importierten Bibliotheken und Ebenen der Lambda-Funktionsversion, die an der Erkenntnis beteiligt waren.

   c. Wenn Sie das Scannen von AWS Lambda Funktionen mit Amazon Inspector aktiviert haben, überprüfen Sie die Ergebnisse von Amazon Inspector, die mit der an der Erkenntnis beteiligten Lambda-Funktion verknüpft sind.

   d. Überprüfen Sie die AWS CloudTrail Protokolle, um den Prinzipal zu identifizieren, der die Funktionsaktualisierung verursacht hat, und stellen Sie sicher, dass die Aktivität autorisiert oder erwartet wurde.

3. Korrigieren Sie die potenziell kompromittierte Lambda-Funktion .

   a. Deaktivieren Sie die Ausführungsauslöser der Lambda-Funktion, die an der Erkenntnis beteiligt sind. Weitere Informationen finden Sie unter DeleteFunctionEventInvokeConfig.

   b. Überprüfen Sie den Lambda-Code und aktualisieren Sie die Bibliotheksimporte und Lambda-Funktionsschichten, um die potenziell verdächtigen Bibliotheken und Schichten zu entfernen.

   c. Mindern Sie die Ergebnisse von Amazon Inspector im Zusammenhang mit der Lambda-Funktion, die an der Erkenntnis beteiligt war.

Verwaltung mehrerer Konten bei Amazon GuardDuty

Wenn Ihre AWS Umgebung über mehrere Konten verfügt, können Sie diese verwalten, indem Sie ein AWS Konto als Administratorkonto festlegen. Sie können diesem Administratorkonto dann andere AWS Konten als Mitgliedskonten zuordnen. Mit diesem angegebenen GuardDuty Administratorkonto können die Schutzpläne konfiguriert werden. GuardDuty Es gibt zwei Möglichkeiten, Konten einem Administratorkonto zuzuordnen: Erstellen Sie eine Organisation, indem Sie verwenden, dass AWS Organizations sowohl das Administratorkonto als auch ein oder mehrere Mitgliedskonten zu dieser Organisation gehören, oder Sie senden eine Einladung an ein AWS Konto über GuardDuty.

GuardDuty empfiehlt die Verwendung der AWS Organizations Methode. Weitere Informationen zum Einrichten einer Organisation finden Sie unter Erstellen einer Organisation im AWS Organizations Benutzerhandbuch.

Verwaltung mehrerer Konten mit AWS Organizations

Wenn das Konto, das Sie als GuardDuty Administratorkonto angeben möchten, Teil einer Organisation ist AWS Organizations, in der Sie dieses Konto als delegierten Administrator der Organisation angeben können. GuardDuty Das Konto, das als delegierter Administrator registriert ist, wird automatisch zum GuardDuty Administratorkonto.

Sie können dieses Administratorkonto verwenden, um jedes Konto AWS-Konto in der Organisation zu aktivieren und zu verwalten GuardDuty , wenn Sie dieses Konto als Mitgliedskonto hinzufügen.

Wenn Sie bereits über ein GuardDuty Administratorkonto mit auf Einladung verknüpften Mitgliedskonten verfügen, können Sie dieses Konto als GuardDuty delegierten Administrator für die Organisation registrieren. Wenn Sie dies tun, bleiben alle derzeit verknüpften Mitgliedskonten Mitglieder, sodass Sie die zusätzlichen Funktionen zur Verwaltung Ihrer GuardDuty Konten bei AWS Organizations in vollem Umfang nutzen können.

Weitere Informationen zur Unterstützung mehrerer Konten innerhalb GuardDuty einer Organisation finden Sie unter GuardDuty Konten verwalten mit AWS Organizations.

Verwalten mehrerer Konten auf Einladung

Wenn die Konten, die Sie zuordnen möchten, nicht zu Ihrer Organisation gehören, können Sie unter ein Administratorkonto angeben GuardDuty und dieses dann verwenden, um andere Benutzer

einzuladen, Mitgliedskonten AWS-Konten zu werden. Wenn das eingeladene Konto die Einladung annimmt, wird dieses Konto zu einem GuardDuty Mitgliedskonto, das dem Administratorkonto zugeordnet ist.

Weitere Informationen zur Unterstützung mehrerer Konten auf Einladung GuardDuty finden Sie unter GuardDuty Konten auf Einladung verwalten.

Grundlegendes zur Beziehung zwischen GuardDuty Administratorkonto und Mitgliedskonten

Wenn Sie GuardDuty in einer Umgebung mit mehreren Konten arbeiten, kann das Administratorkonto bestimmte Aspekte von im Namen der GuardDuty Mitgliedskonten verwalten. Das Administratorkonto kann die folgenden Hauptfunktionen ausführen:

- Hinzufügen und Entfernen zugehöriger Mitgliedskonten. Der Prozess, mit dem dies durchgeführt wird, unterscheidet sich je nachdem, ob die Konten über Organisationen oder auf Einladung zugeordnet werden.
- Den Status der zugehörigen Mitgliedskonten verwalten, einschließlich Aktivierung und Sperrung. GuardDuty GuardDuty

  > **Note**
  >
  > Delegierte Administratorkonten werden mit AWS Organizations automatischer Aktivierung GuardDuty in Konten verwaltet, die als Mitglieder hinzugefügt wurden.

- Passen Sie die Ergebnisse innerhalb des GuardDuty Netzwerks an, indem Sie Unterdrückungsregeln, Listen vertrauenswürdiger IP-Adressen und Bedrohungslisten erstellen und verwalten. Mitgliedskonten verlieren in einer Umgebung mit mehreren Konten den Zugriff auf diese Funktionen.

In der folgenden Tabelle wird die Beziehung zwischen GuardDuty Administratorkonten und Mitgliedskonten detailliert beschrieben.

In dieser Tabelle:

- Selbst — Ein Konto kann die aufgelistete Aktion nur für sein eigenes Konto ausführen.
- Beliebig — Ein Konto kann die aufgelistete Aktion für jedes zugehörige Konto ausführen.

- Alle — Ein Konto kann die aufgelistete Aktion ausführen und sie gilt für alle zugehörigen Konten. In der Regel handelt es sich bei dem Konto, das diese Aktion ausführt, um ein GuardDuty designiertes Administratorkonto

Tabellenzellen mit einem Bindestrich (—) weisen darauf hin, dass das Konto die aufgelistete Aktion nicht ausführen kann.

Action (Aktion)	Durch AWS Organizations		Auf Einladung	
	Delegiertes GuardDuty Administratorkonto	Zugeordnetes Mitgliedskonto	Delegiertes GuardDuty Administratorkonto	Zugeordnetes Mitgliedskonto
Enable GuardDuty	Any	–	Self	Self
Enable GuardDuty automatically for the entire organization (`ALL`, `NEW`, `NONE`)	All	–	–	–
View all Organizations member accounts regardless of GuardDuty status	Any	–	–	–
Generate sample findings	Self	Self	Self	Self

View all GuardDuty findings	Any	Self	Any	Self
Archive GuardDuty findings	Any	–	Any	–
Apply suppressi on rules	All	–	All	–
Create trusted IP list or threat lists	All	–	All	–
Update trusted IP list or threat lists	All	–	All	–
Delete trusted IP list or threat lists	All	–	All	–
Set EventBrid ge notification frequency	All	–	All	Self
Set Amazon S3 location for exporting findings	All	–	All	Self
Enable one or more optional protection plans for the entire organization (`ALL`, `NEW`, `NONE`)	All	–	–	–

Enable any GuardDuty protection plan for individual accounts	Any	–	Any	Self
Disassociate a member account	Any	–	Any	–
Disassociate from an administrator account account	–	Self[#]	–	Self
Delete a disassociated member account	Any	–	Any	–
Suspend GuardDuty	Any[*]	–	Any[*]	–
Disable GuardDuty	Any[*]	–	Any[*]	–

- # Zeigt an, dass das Konto diese Aktion nur ausführen kann, wenn das delegierte GuardDuty Administratorkonto nicht die automatische Aktivierung für ALL die Organisationsmitglieder eingerichtet hat.
- * Zeigt an, dass diese Aktion für alle zugehörigen Konten ausgeführt werden muss, bevor sie für dieses Konto ausgeführt wird. Nachdem Sie die Zuordnung dieser Konten aufgehoben haben, müssen Sie sie löschen. Weitere Informationen zur Ausführung dieser Aufgaben in Ihrer Organisation finden Sie unter Aufrechterhaltung Ihrer Organisation innerhalb GuardDuty.

GuardDuty Konten verwalten mit AWS Organizations

Wenn Sie es GuardDuty zusammen mit einer AWS Organisation verwenden, kann das Verwaltungskonto dieser Organisation jedes Konto innerhalb der Organisation als GuardDuty delegiertes Administratorkonto festlegen. Für dieses Administratorkonto GuardDuty wird es

automatisch nur im angegebenen Konto aktiviert. AWS-Region Dieses Konto ist außerdem berechtigt, alle Konten in der Organisation in dieser Region zu aktivieren und zu verwalten GuardDuty . Das Administratorkonto kann die Mitglieder dieser Organisation anzeigen und Mitglieder zu dieser AWS Organisation hinzufügen.

Wenn Sie bereits ein GuardDuty Administratorkonto mit verknüpften Mitgliedskonten auf Einladung eingerichtet haben und die Mitgliedskonten derselben Organisation angehören, ändert sich ihr Typ von „Auf Einladung“ zu „Über Organizations“, wenn Sie ein delegiertes GuardDuty Administratorkonto für Ihre Organisation einrichten. Wenn ein delegiertes GuardDuty Administratorkonto zuvor Mitglieder auf Einladung hinzugefügt hat, die nicht derselben Organisation angehören, bleibt ihr Typ „Auf Einladung“ erhalten. In beiden Fällen handelt es sich bei den zuvor hinzugefügten Konten um Mitgliedskonten, die dem delegierten GuardDuty Administratorkonto der Organisation zugeordnet sind.

Sie können weiterhin Konten als Mitglieder hinzufügen, auch wenn sich diese außerhalb Ihrer Organisation befinden. Weitere Informationen finden Sie unter Hinzufügen und verwalten von Konten auf Einladung oder Benennen Sie ein delegiertes GuardDuty Administratorkonto und verwalten Sie Mitglieder mithilfe der Konsole GuardDuty .

Inhalt

Überlegungen und Empfehlungen bei der Benennung eines delegierten Administratorkontos GuardDuty

Die folgenden Überlegungen und Empfehlungen können Ihnen helfen zu verstehen, wie ein delegiertes GuardDuty Administratorkonto funktioniert in GuardDuty:

Ein delegiertes GuardDuty Administratorkonto kann maximal 50.000 Mitglieder verwalten.

Es gibt ein Limit von 50.000 Mitgliedskonten pro delegiertem GuardDuty Administratorkonto. Dies schließt Mitgliedskonten ein, die über die Einladung des Administratorkontos zum Beitritt zu ihrer Organisation hinzugefügt wurden, AWS Organizations oder solche, die die Einladung des GuardDuty Administratorkontos angenommen haben. In Ihrer AWS Organisation kann es jedoch mehr als 50.000 Konten geben.

Wenn Sie das Limit von 50.000 Mitgliedskonten überschreiten, erhalten Sie eine Benachrichtigung von CloudWatch AWS Health Dashboard, und eine E-Mail an das angegebene delegierte GuardDuty Administratorkonto.

Ein delegiertes GuardDuty Administratorkonto ist Regional.

Im Gegensatz AWS Organizations dazu GuardDuty handelt es sich um einen Regionaldienst. Die delegierten GuardDuty Administratorkonten und ihre Mitgliedskonten müssen AWS Organizations in jeder gewünschten Region, in der Sie sie GuardDuty aktiviert haben, hinzugefügt werden. Wenn das Organisationsverwaltungskonto ein delegiertes GuardDuty Administratorkonto nur für USA Ost (Nord-Virginia) festlegt, verwaltet das delegierte GuardDuty Administratorkonto nur Mitgliedskonten, die der Organisation in dieser Region hinzugefügt wurden. Weitere Informationen zur Funktionsparität in Regionen, in denen GuardDuty sie verfügbar ist, finden Sie unter. Regionen und Endpunkte

Sonderfälle für Opt-in-Regionen

- Wenn sich ein delegiertes GuardDuty Administratorkonto von einer Opt-in-Region abmeldet, GuardDuty kann es für kein Mitgliedskonto in der Organisation aktiviert werden, das derzeit deaktiviert ist, auch wenn in Ihrer Organisation die Konfiguration für die GuardDuty automatische Aktivierung entweder auf nur neue Mitgliedskonten (`NEWALL`) oder auf alle Mitgliedskonten () eingestellt ist. GuardDuty Informationen zur Konfiguration Ihrer Mitgliedskonten finden Sie im Navigationsbereich der GuardDuty Konsole unter Konten oder verwenden Sie die API. ListMembers
- Wenn Sie mit der Konfiguration für GuardDuty automatische Aktivierung arbeiten, stellen Sie sicher`NEW`, dass die folgende Reihenfolge eingehalten wird:

  1. Die Mitgliedskonten melden sich für eine Opt-in-Region an.
  2. Fügen Sie die Mitgliedskonten Ihrer Organisation in hinzu. AWS Organizations

  Wenn Sie die Reihenfolge dieser Schritte ändern, funktioniert die Einstellung für die GuardDuty automatische Aktivierung mit `NEW` in der jeweiligen Opt-in-Region nicht mehr, da das

Mitgliedskonto für die Organisation nicht mehr neu ist. GuardDuty bietet zwei alternative Lösungen:

- Stellen Sie die Konfiguration für die GuardDuty automatische Aktivierung auf ein`ALL`, die neue und bestehende Mitgliedskonten einschließt. In diesem Fall ist die Reihenfolge dieser Schritte nicht relevant.
- Wenn ein Mitgliedskonto bereits Teil Ihrer Organisation ist, verwalten Sie die GuardDuty Konfiguration für dieses Konto individuell in der jeweiligen Opt-in-Region mithilfe der GuardDuty Konsole oder der API.

Es wird empfohlen, dass eine AWS Organisation für alle über dasselbe delegierte GuardDuty Administratorkonto verfügt. AWS-Regionen

Wir empfehlen Ihnen, Ihrer Organisation AWS-Regionen in allen Bereichen, die Sie aktiviert haben, dasselbe delegierte GuardDuty Administratorkonto zuzuweisen. GuardDuty Wenn Sie in einer Region ein Konto als delegiertes GuardDuty Administratorkonto festlegen, wird empfohlen, dasselbe Konto als delegiertes GuardDuty Administratorkonto in allen anderen Regionen zu verwenden.

Sie können jederzeit ein neues delegiertes GuardDuty Administratorkonto einrichten. Weitere Informationen zum Entfernen des vorhandenen delegierten GuardDuty Administratorkontos finden Sie unter. Ändern des delegierten GuardDuty Administratorkontos

Es wird nicht empfohlen, das Verwaltungskonto Ihrer Organisation als delegiertes GuardDuty Administratorkonto festzulegen.

Das Verwaltungskonto Ihrer Organisation kann das delegierte GuardDuty Administratorkonto sein. Die bewährten AWS -Sicherheitsmethoden folgen jedoch dem Prinzip der geringsten Berechtigung und empfehlen diese Konfiguration nicht.

Durch das Ändern eines delegierten GuardDuty Administratorkontos werden Mitgliedskonten nicht deaktiviert GuardDuty .

Wenn Sie ein delegiertes GuardDuty Administratorkonto entfernen, werden alle Mitgliedskonten GuardDuty entfernt, die diesem delegierten GuardDuty Administratorkonto zugeordnet sind. GuardDuty bleibt weiterhin für all diese Mitgliedskonten aktiviert.

Für die Benennung eines delegierten GuardDuty Administratorkontos sind Berechtigungen erforderlich

Wenn Sie ein delegiertes GuardDuty Administratorkonto delegieren, müssen Sie über Berechtigungen zum Aktivieren GuardDuty sowie für bestimmte API-Aktionen verfügen. AWS Organizations Sie können die folgende Anweisung am Ende einer vorhandenen IAM-Richtlinie hinzufügen, um diese Berechtigungen zu erteilen:

```
{
    "Sid": "PermissionsForGuardDutyAdmin",
    "Effect": "Allow",
    "Action": [
        "guardduty:EnableOrganizationAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
}
```

Wenn Sie Ihr AWS Organizations Verwaltungskonto als GuardDuty delegiertes GuardDuty Administratorkonto festlegen möchten, benötigt `CreateServiceLinkedRole` diese Entität außerdem Berechtigungen zur Initialisierung. GuardDuty Fügen Sie dazu der IAM-Richtlinie die folgende Anweisung hinzu und ersetzen Sie *111122223333* durch die ID des AWS-Konto Verwaltungskontos Ihrer Organisation:

```
{
 "Sid": "PermissionsToEnableGuardDuty"
 "Effect": "Allow",
 "Action": [
  "iam:CreateServiceLinkedRole"
 ],
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty",
 "Condition": {
  "StringLike": {
```

```
    "iam:AWSServiceName": "guardduty.amazonaws.com"
   }
  }
 }
```

Benennen Sie ein delegiertes GuardDuty Administratorkonto und verwalten Sie Mitglieder mithilfe der Konsole GuardDuty

Inhalt

Schritt 1 — Benennen Sie ein delegiertes GuardDuty Administratorkonto für Ihre Organisation

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Verwenden Sie zur Anmeldung die Anmeldeinformationen für das Verwaltungskonto Ihrer AWS Organizations -Organisation.
2. Wenn Sie das Verwaltungskonto bereits aktiviert GuardDuty haben, überspringen Sie diesen Schritt und folgen Sie dem nächsten Schritt.

   Wenn Sie es GuardDuty noch nicht aktiviert haben, wählen Sie Erste Schritte aus und legen Sie dann auf der Seite Willkommen GuardDuty bei ein delegiertes GuardDuty Administratorkonto fest.

   > **Note**
   >
   > Das Verwaltungskonto muss über die GuardDuty serviceverknüpfte Rolle (SLR) verfügen, damit das delegierte GuardDuty Administratorkonto in diesem Konto aktiviert und verwaltet werden kann. GuardDuty Sobald Sie das Verwaltungskonto GuardDuty in einer Region aktiviert haben, wird dieses SLR automatisch erstellt.
3. Führen Sie diesen Schritt aus, nachdem Sie die Aktivierung GuardDuty für das Verwaltungskonto vorgenommen haben. Wählen Sie im Navigationsbereich der GuardDuty Konsole Einstellungen

aus. Geben Sie auf der Seite Einstellungen die 12-stellige AWS-Konto ID des Kontos ein, das Sie als delegiertes GuardDuty Administratorkonto für die Organisation festlegen möchten.

Stellen Sie sicher, dass Sie GuardDuty die Aktivierung für Ihr neu benanntes delegiertes GuardDuty Administratorkonto vornehmen, da es sonst keine Aktion ausführen kann.

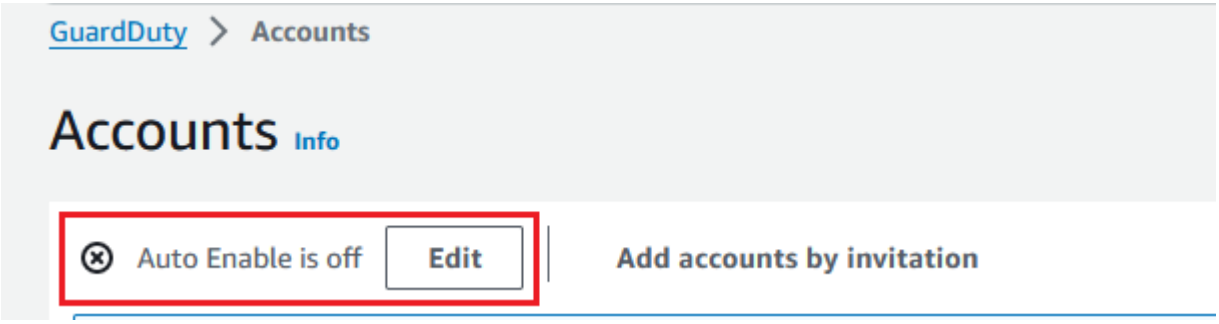
4. Wählen Sie Delegieren.
5. (Empfohlen) Wiederholen Sie den vorherigen Schritt, um das delegierte GuardDuty Administratorkonto für jedes Konto festzulegen, das Sie AWS-Region aktiviert haben. GuardDuty

Schritt 2 — Konfiguration der Einstellungen für die automatische Aktivierung für Ihr Unternehmen

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Verwenden Sie die Anmeldeinformationen des GuardDuty Administratorkontos, um sich anzumelden.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.

   Auf der Seite Konten finden Sie Konfigurationsoptionen für das GuardDuty Administratorkonto zur automatischen Aktivierung GuardDuty sowie optionale Schutzpläne für die Mitgliedskonten, die zur Organisation gehören.
3. Um die vorhandenen Einstellungen für die automatische Aktivierung zu aktualisieren, wählen Sie Bearbeiten.



Diese Unterstützung kann konfiguriert werden, GuardDuty ebenso wie alle unterstützten optionalen Schutzpläne in Ihrem. AWS-Region Sie können im Namen Ihrer Mitgliedskonten eine der folgenden Konfigurationsoptionen auswählen: GuardDuty

- Für alle Konten aktivieren (**`ALL`**) — Wählen Sie diese Option, um die entsprechende Option für alle Konten in einer Organisation zu aktivieren. Dazu gehören neue Konten, die der

Organisation beitreten, und Konten, die möglicherweise gesperrt oder aus der Organisation entfernt wurden. Dazu gehört auch das delegierte GuardDuty Administratorkonto.

> **Note**
>
> Es kann bis zu 24 Stunden dauern, bis die Konfiguration für alle Mitgliedskonten aktualisiert ist.

- Automatische Aktivierung für neue Konten (**`NEW`**) — Wählen Sie aus, GuardDuty ob die optionalen Schutzpläne nur für neue Mitgliedskonten automatisch aktiviert werden sollen, wenn diese Ihrer Organisation beitreten.
- Nicht aktivieren (**`NONE`**) — Wählen Sie diese Option, um zu verhindern, dass die entsprechende Option für neue Konten in Ihrer Organisation aktiviert wird. In diesem Fall verwaltet das GuardDuty Administratorkonto jedes Konto einzeln.

  Wenn Sie die Einstellung für die automatische Aktivierung von `ALL` oder `NEW` auf aktualisieren`NONE`, deaktiviert diese Aktion nicht die entsprechende Option für Ihre vorhandenen Konten. Diese Konfiguration gilt für die neuen Konten, die der Organisation beitreten. Nachdem Sie die Einstellungen für die automatische Aktivierung aktualisiert haben, wird die entsprechende Option für kein neues Konto aktiviert sein.

> **Note**
>
> Wenn sich ein delegiertes GuardDuty Administratorkonto von einer Opt-in-Region abmeldet, GuardDuty kann es für kein Mitgliedskonto in der Organisation aktiviert werden, das derzeit deaktiviert ist, auch wenn in Ihrer Organisation die Konfiguration für die GuardDuty automatische Aktivierung entweder auf nur neue Mitgliedskonten (`NEWALL`) oder auf alle Mitgliedskonten () eingestellt ist. GuardDuty Informationen zur Konfiguration Ihrer Mitgliedskonten finden Sie im Navigationsbereich der GuardDuty Konsole unter Konten oder verwenden Sie die API. ListMembers

4. Wählen Sie Änderungen speichern aus.
5. (Optional) Wenn Sie in jeder Region dieselben Einstellungen verwenden möchten, aktualisieren Sie Ihre Einstellungen in jeder der unterstützten Regionen separat.

Einige der optionalen Schutzpläne sind möglicherweise nicht überall verfügbar, AWS-Regionen wo sie verfügbar GuardDuty sind. Weitere Informationen finden Sie unter Regionen und Endpunkte.

Schritt 3 – Konten als Mitglieder zu Ihrer Organisation hinzufügen

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Verwenden Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto, um sich anzumelden.

2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.

   In der Kontentabelle werden alle Konten angezeigt, die entweder Über Organisationen (AWS Organizations) oder Auf Einladung hinzugefügt wurden. Wenn ein Mitgliedskonto nicht mit dem GuardDuty Administratorkonto der Organisation verknüpft ist, lautet der Status dieses Mitgliedskontos Kein Mitglied.

3. Wählen Sie eine oder mehrere Konto-IDs aus, die Sie als Mitglieder hinzufügen möchten. Diese Konto-IDs müssen den Typ Über Organisationen haben.

   Konten, die auf Einladung hinzugefügt werden, gehören nicht zu Ihrer Organisation. Sie können solche Konten einzeln verwalten. Weitere Informationen finden Sie unter Verwalten von Konten auf Einladung.

4. Wählen Sie das Drop-Down Aktionen und dann Mitglied hinzufügen aus. Nachdem Sie dieses Konto als Mitglied hinzugefügt haben, gilt die GuardDuty Konfiguration für die automatische Aktivierung. Je nach den Einstellungen in kann the section called “Schritt 1 — Benennen Sie ein delegiertes GuardDuty Administratorkonto für Ihre Organisation” sich die GuardDuty Konfiguration dieser Konten ändern.

5. Sie können den Abwärtspfeil in der Spalte Status auswählen, um die Konten nach dem Status Kein Mitglied zu sortieren, und dann jedes Konto auswählen, das in der aktuellen Region nicht GuardDuty aktiviert wurde.

   Wenn noch keines der in der Kontentabelle aufgelisteten Konten als Mitglied hinzugefügt wurde, können Sie es GuardDuty in der aktuellen Region für alle Organisationskonten aktivieren. Wählen Sie im Banner oben auf der Seite Aktivieren aus. Durch diese Aktion wird automatisch die GuardDuty Konfiguration „Automatische Aktivierung“ aktiviert, sodass sie für jedes neue Konto aktiviert GuardDuty wird, das der Organisation beitritt.

6. Wählen Sie Bestätigen, um die Konten als Mitglieder hinzuzufügen. Diese Aktion ist auch GuardDuty für alle ausgewählten Konten aktiviert. Der Status für die eingeladenen Konten ändert sich in Aktiviert.
7. (Empfohlen) Wiederholen Sie diese Schritte in jedem Schritt AWS-Region. Dadurch wird sichergestellt, dass das delegierte GuardDuty Administratorkonto Ergebnisse und andere Konfigurationen für Mitgliedskonten in allen Regionen verwalten kann, in denen Sie die GuardDuty Aktivierung aktiviert haben.

   Die automatische Aktivierungsfunktion ist GuardDuty für alle future Mitglieder Ihrer Organisation aktiviert. Auf diese Weise kann Ihr delegiertes GuardDuty Administratorkonto alle neuen Mitglieder verwalten, die innerhalb der Organisation erstellt wurden oder der Organisation hinzugefügt werden. Wenn die Anzahl der Mitgliedskonten das Limit von 50.000 erreicht, wird die Funktion zur automatischen Aktivierung automatisch deaktiviert. Wenn Sie ein Mitgliedskonto entfernen und die Gesamtzahl der Mitglieder auf weniger als 50.000 sinkt, wird die Funktion zur automatischen Aktivierung wieder aktiviert.

(Optional) Schritt 4 — Schutzpläne für einzelne Konten konfigurieren

Auf der Seite Konten können Sie Schutzpläne für einzelne Konten konfigurieren.

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Verwenden Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Wählen Sie das Konto aus, für das Sie einen Schutzplan konfigurieren möchten. Wiederholen Sie die folgenden Schritte für jeden Schutzplan, den Sie konfigurieren möchten:

   a. Wählen Sie Schutzpläne bearbeiten aus.

   b. Wählen Sie aus der Liste der Schutzpläne einen Schutzplan aus, den Sie konfigurieren möchten.

   c. Wählen Sie eine der Aktionen aus, die Sie für diesen Schutzplan ausführen möchten, und klicken Sie dann auf Bestätigen.

   d. Für das ausgewählte Konto wird in der Spalte, die dem konfigurierten Schutzplan entspricht, die aktualisierte Konfiguration als Aktiviert oder Nicht aktiviert angezeigt.

Benennen eines GuardDuty delegierten GuardDuty Administratorkontos und Verwalten von Mitgliedern mithilfe der API

Inhalt

Schritt 1 — Benennen Sie ein delegiertes GuardDuty Administratorkonto für Ihre Organisation AWS

1. Führen Sie die Ausführung enableOrganizationAdminAccountmit den Anmeldeinformationen AWS-Konto des Verwaltungskontos der Organisation aus.
   - Alternativ können Sie AWS Command Line Interface dies verwenden. Der folgende AWS CLI Befehl bestimmt ein delegiertes GuardDuty Administratorkonto nur für Ihre aktuelle Region. Führen Sie den folgenden AWS CLI Befehl aus und achten Sie darauf, *111111111* durch die AWS-Konto ID des Kontos zu ersetzen, das Sie als delegiertes Administratorkonto festlegen möchten: GuardDuty

     ```
     aws guardduty enable-organization-admin-account --admin-account-id 111111111111
     ```

     Um das delegierte GuardDuty Administratorkonto für andere Regionen festzulegen, geben Sie die Region im Befehl an. AWS CLI Das folgende Beispiel zeigt, wie ein delegiertes GuardDuty Administratorkonto in US West (Oregon) aktiviert wird. Stellen Sie sicher, dass Sie *us-west-2* durch die Region ersetzen, für die Sie das GuardDuty delegierte GuardDuty Administratorkonto zuweisen möchten.

     ```
     aws guardduty enable-organization-admin-account --admin-account-id 111111111111
      --region us-west-2
     ```

     Informationen darüber, AWS-Regionen wo verfügbar GuardDuty ist, finden Sie unter. Regionen und Endpunkte

   Wenn GuardDuty es für Ihr delegiertes GuardDuty Administratorkonto nicht aktiviert ist, kann es keine Aktion ausführen. Falls dies noch nicht geschehen ist, stellen Sie sicher, dass Sie

die Aktivierung GuardDuty für das neu benannte delegierte GuardDuty Administratorkonto vorgenommen haben.

2. (Empfohlen) Wiederholen Sie den vorherigen Schritt, um das delegierte GuardDuty Administratorkonto AWS-Region in allen Bereichen festzulegen, die Sie aktiviert haben. GuardDuty

Schritt 2 – Konfiguration der Einstellungen für die automatische Aktivierung für die Organisation

1. 1. Führen Sie den Vorgang UpdateOrganizationConfigurationmithilfe der Anmeldeinformationen des delegierten GuardDuty Administratorkontos aus, um in dieser Region automatisch optionale Schutzpläne für Ihr Unternehmen zu konfigurieren GuardDuty

   Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ - Konsole.

   > **Note**
   >
   > Informationen zu den verschiedenen Konfigurationen für die automatische Aktivierung finden Sie unter autoEnableOrganizationMitglieder.

   2. Um die Einstellungen für die automatische Aktivierung für einen der unterstützten optionalen Schutzpläne in Ihrer Region festzulegen, folgen Sie den Schritten in den entsprechenden Dokumentationsabschnitten der einzelnen Schutzpläne.
   3. Sie können die Einstellungen für Ihre Organisation in der aktuellen Region überprüfen. Führen Sie describeOrganizationConfiguration. Stellen Sie sicher, dass Sie die Melder-ID des delegierten GuardDuty Administratorkontos angeben.

   > **Note**
   >
   > Die Aktualisierung der Konfiguration aller Mitgliedskonten kann bis zu 24 Stunden dauern.

   - 1. Führen Sie alternativ den folgenden AWS CLI Befehl aus, um die Einstellungen so festzulegen, dass GuardDuty in dieser Region automatisch neue Konten (`NEW`),

die der Organisation beitreten, alle Konten (`ALL`) oder keines der Konten (`NONE`) in der Organisation aktiviert oder deaktiviert werden. Weitere Informationen finden Sie unter autoEnableOrganizationMitglieder. Je nach Ihren Einstellungen müssen Sie möglicherweise `NEW` durch `ALL` oder `NONE` ersetzen. Wenn Sie den Schutzplan mit konfigurierenALL, wird der Schutzplan auch für das delegierte GuardDuty Administratorkonto aktiviert. Stellen Sie sicher, dass Sie die Melder-ID des delegierten GuardDuty Administratorkontos angeben, das die Organisationskonfiguration verwaltet.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
```

2. Sie können die Einstellungen für Ihre Organisation in der aktuellen Region überprüfen. Führen Sie den folgenden AWS CLI Befehl aus, indem Sie die Detektor-ID des delegierten GuardDuty Administratorkontos verwenden.

```
aws guardduty describe-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0
```

2. (Empfohlen) Wiederholen Sie die vorherigen Schritte in jeder Region, indem Sie die Detektor-ID für das delegierte GuardDuty Administratorkonto verwenden.

> **Note**
>
> Wenn sich ein delegiertes GuardDuty Administratorkonto von einer Opt-in-Region abmeldet, GuardDuty kann es für kein Mitgliedskonto in der Organisation aktiviert werden, das derzeit deaktiviert ist, auch wenn in Ihrer Organisation die Konfiguration für die GuardDuty automatische Aktivierung entweder auf nur neue Mitgliedskonten (`NEWALL`) oder auf alle Mitgliedskonten () eingestellt ist. GuardDuty Informationen zur Konfiguration Ihrer Mitgliedskonten finden Sie im Navigationsbereich der GuardDuty Konsole unter Konten oder verwenden Sie die API. ListMembers

Schritt 3 – Konten als Mitglieder zu Ihrer Organisation hinzufügen

- Verwenden Sie für die Ausführung CreateMembersdie Anmeldeinformationen des delegierten GuardDuty Administratorkontos, das Sie im vorherigen Schritt angegeben haben.

  Sie müssen die Regional Detector-ID des delegierten GuardDuty Administratorkontos und die Kontodetails (AWS-Konto IDs und entsprechende E-Mail-Adressen) der Konten angeben, die Sie als GuardDuty Mitglieder hinzufügen möchten. Sie können mit dieser API-Operation ein oder mehrere Mitglieder erstellen.

  Wenn Sie CreateMembers in Ihrer Organisation aktiv sind, gelten die Einstellungen für die automatische Aktivierung für neue Mitglieder, sobald neue Mitgliedskonten Ihrer Organisation beitreten. Wenn Sie CreateMembers mit einem bestehenden Mitgliedskonto arbeiten, gilt die Organisationskonfiguration auch für die vorhandenen Mitglieder. Dies könnte die aktuelle Konfiguration der vorhandenen Mitgliedskonten ändern.

  Führen Sie ListAccountsdie AWS Organizations API-Referenz aus, um alle Konten in der AWS Organisation anzuzeigen.

  > **Important**
  >
  > Wenn Sie ein Konto als GuardDuty Mitglied hinzufügen, wird es automatisch in dieser Region GuardDuty aktiviert. Es gibt eine Ausnahme für das Organisationsverwaltungskonto. Bevor das Verwaltungskonto als GuardDuty Mitglied hinzugefügt werden kann, muss es GuardDuty aktiviert worden sein.

- Alternativ können Sie verwenden AWS Command Line Interface. Führen Sie den folgenden AWS CLI -Befehl aus und stellen Sie sicher, dass Sie Ihre eigene gültige Detektor-ID und die mit der AWS-Konto -ID verknüpfte E-Mail-Adresse verwenden.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

  ```
  aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  account-details AccountId=111122223333,Email=guardduty-member-name@amazon.com
  ```

Sie können eine Liste aller Organisationsmitglieder anzeigen, indem Sie den folgenden AWS CLI Befehl ausführen:

```
aws organizations list-accounts
```

Nachdem Sie dieses Konto als Mitglied hinzugefügt haben, gilt die GuardDuty Konfiguration für die automatische Aktivierung.

Aufrechterhaltung Ihrer Organisation innerhalb GuardDuty

Als delegiertes GuardDuty Administratorkonto sind Sie dafür verantwortlich, die Konfiguration GuardDuty und die optionalen Schutzpläne für alle Konten in Ihrer Organisation in allen unterstützten Konten aufrechtzuerhalten. AWS-Region In den folgenden Abschnitten finden Sie die Optionen zur Beibehaltung des Konfigurationsstatus der optionalen Schutzpläne GuardDuty oder der zugehörigen optionalen Schutzpläne:

Um den Konfigurationsstatus Ihrer gesamten Organisation in jeder Region aufrechtzuerhalten

- Legen Sie mithilfe der GuardDuty Konsole Einstellungen für die automatische Aktivierung für die gesamte Organisation fest — Sie können die GuardDuty automatische Aktivierung entweder für alle (`ALL`) Mitglieder der Organisation oder für neue (`NEW`) Mitglieder, die der Organisation beitreten, aktivieren oder festlegen, dass (`NONE`) keines der Mitglieder der Organisation automatisch aktiviert wird.

  Sie können auch dieselben oder unterschiedliche Einstellungen für alle darin enthaltenen Schutzpläne konfigurieren. GuardDuty

  Es kann bis zu 24 Stunden dauern, bis die Konfiguration für alle Mitgliedskonten in der Organisation aktualisiert ist.
- Aktualisieren Sie die Einstellungen für die automatische Aktivierung mithilfe von API — Run UpdateOrganizationConfiguration, um die automatische Konfiguration GuardDuty und die optionalen Schutzpläne für das Unternehmen zu konfigurieren. Wenn Sie ausführen CreateMembers, um neue Mitgliedskonten in Ihrer Organisation hinzuzufügen, werden die konfigurierten Einstellungen automatisch angewendet. Wenn Sie CreateMembers mit einem vorhandenen Mitgliedskonto arbeiten, gilt die Organisationskonfiguration auch für die vorhandenen Mitglieder. Dies könnte die aktuelle Konfiguration der vorhandenen Mitgliedskonten ändern.

Um alle Konten in Ihrer Organisation anzuzeigen, führen Sie ListAccountsden Befehl AWS Organizations API-Referenz aus.

Um den Konfigurationsstatus für Mitgliedskonten in jeder Region einzeln beizubehalten

- Um alle Konten in Ihrer Organisation anzuzeigen, führen Sie ListAccountsden Befehl AWS Organizations API-Referenz aus.
- Wenn Sie möchten, dass ausgewählte Mitgliedskonten einen anderen Konfigurationsstatus haben, führen Sie den Vorgang UpdateMemberDetectorsfür jedes Mitgliedskonto einzeln aus.

  Sie können die GuardDuty Konsole verwenden, um dieselbe Aufgabe auszuführen, indem Sie in der GuardDuty Konsole zur Seite Konten navigieren.

  Informationen zur Aktivierung von Schutzplänen für einzelne Konten mithilfe der Konsole oder der API finden Sie auf der Konfigurationsseite für den entsprechenden Schutzplan.

Ändern des delegierten GuardDuty Administratorkontos

Sie können das delegierte GuardDuty Administratorkonto für Ihre Organisation in jeder Region ändern und dann in jeder Region einen neuen Administrator delegieren. Um die Sicherheit der Mitgliedskonten Ihrer Organisation in einer Region aufrechtzuerhalten, benötigen Sie in dieser Region ein delegiertes GuardDuty Administratorkonto.

Bestehendes delegiertes GuardDuty Administratorkonto wird entfernt

Schritt 1 — Um ein vorhandenes delegiertes GuardDuty Administratorkonto in jeder Region zu entfernen

1. Führen Sie als vorhandenes delegiertes GuardDuty Administratorkonto alle Mitgliedskonten auf, die Ihrem Administratorkonto zugeordnet sind. Führen Sie ListMembersmit`OnlyAssociated=false`.
2. Wenn die Einstellung Automatische Aktivierung für GuardDuty oder einen der optionalen Schutzpläne auf gesetzt ist, führen Sie den Befehl aus`ALL`, UpdateOrganizationConfigurationum die Organisationskonfiguration entweder auf `NEW` oder `NONE` zu aktualisieren. Diese Aktion verhindert, dass ein Fehler auftritt, wenn Sie im nächsten Schritt die Verknüpfung aller Mitgliedskonten aufheben.

3. Führen Sie aus DisassociateMembers, um die Zuordnung aller Mitgliedskonten aufzuheben, die dem Administratorkonto zugeordnet sind.
4. Ausführen DeleteMembers, um die Verknüpfungen zwischen dem Administratorkonto und den Mitgliedskonten zu löschen.
5. Führen Sie als Organisationsverwaltungskonto aus, DisableOrganizationAdminAccountum das vorhandene delegierte GuardDuty Administratorkonto zu entfernen.
6. Wiederholen Sie diese Schritte in allen Bereichen, in AWS-Region denen Sie über dieses delegierte GuardDuty Administratorkonto verfügen.

Schritt 2 — So heben Sie die Registrierung eines bestehenden delegierten GuardDuty Administratorkontos in AWS Organizations (einmalige globale Aktion) auf

- Führen Sie DeregisterDelegatedAdministratordie AWS Organizations API-Referenz aus, um das bestehende delegierte GuardDuty Administratorkonto in abzumelden. AWS Organizations

  Alternativ können Sie den folgenden AWS CLI Befehl ausführen:

  ```
  aws organizations deregister-delegated-administrator --account-id 111122223333 --
  service-principal guardduty.amazonaws.com
  ```

  Stellen Sie sicher, dass Sie *111122223333* durch das vorhandene delegierte Administratorkonto ersetzen. GuardDuty

  Nachdem Sie das alte delegierte GuardDuty Administratorkonto abgemeldet haben, können Sie es dem neuen delegierten Administratorkonto als Mitgliedskonto hinzufügen. GuardDuty

Benennen eines neuen delegierten GuardDuty Administratorkontos in jeder Region

1. Weisen Sie in jeder Region ein neues delegiertes GuardDuty Administratorkonto zu, indem Sie eine der folgenden Zugriffsmethoden verwenden:

   - GuardDuty Konsole verwenden —. Schritt 1 — Benennen Sie ein delegiertes GuardDuty Administratorkonto für Ihre Organisation
   - GuardDuty API verwenden —Schritt 1 — Benennen Sie ein delegiertes GuardDuty Administratorkonto für Ihre Organisation AWS.

2. Führen Sie den DescribeOrganizationConfigurationBefehl aus, um die aktuelle Konfiguration für die automatische Aktivierung für Ihre Organisation anzuzeigen.

> **Important**
>
> Bevor Sie dem neuen delegierten GuardDuty Administratorkonto Mitglieder hinzufügen, müssen Sie die Konfiguration für die automatische Aktivierung für Ihre Organisation überprüfen. Diese Konfiguration ist spezifisch für das neue delegierte GuardDuty Administratorkonto und die ausgewählte Region und bezieht sich nicht auf. AWS Organizations Wenn Sie (ein neues oder ein vorhandenes) Mitgliedskonto einer Organisation unter dem neuen delegierten GuardDuty Administratorkonto hinzufügen, gilt die automatische Aktivierungskonfiguration des neuen delegierten GuardDuty Administratorkontos zum Zeitpunkt der Aktivierung GuardDuty oder eines seiner optionalen Schutzpläne.

Verwenden Sie eine der folgenden Zugriffsmethoden, um diese Organisationskonfiguration für das neue delegierte GuardDuty Administratorkonto zu ändern:

- GuardDuty Konsole verwenden —Schritt 2 — Konfiguration der Einstellungen für die automatische Aktivierung für Ihr Unternehmen.
- GuardDuty API verwenden —Schritt 2 – Konfiguration der Einstellungen für die automatische Aktivierung für die Organisation.

GuardDuty Konten auf Einladung verwalten

Um Konten außerhalb Ihrer Organisation zu verwalten, können Sie die Legacy-Einladungsmethode verwenden. Wenn Sie diese Methode verwenden, wird Ihr Konto als Administratorkonto designiert, wenn ein anderes Konto Ihre Einladung annimmt, ein Mitgliedskonto zu werden.

Wenn es sich bei Ihrem Konto nicht um ein Administratorkonto handelt, können Sie eine Einladung von einem anderen Konto annehmen. In diesem Fall wird Ihr Konto ein Mitgliedskonto. Ein AWS Konto kann nicht gleichzeitig GuardDuty Administratorkonto und Mitgliedskonto sein.

Wenn Sie eine Einladung von einem Konto annehmen, können Sie keine Einladung von einem anderen Konto annehmen. Um eine Einladung von einem anderen Konto anzunehmen, müssen Sie zunächst die Verbindung zwischen Ihrem Konto und dem vorhandenen Administratorkonto trennen.

Alternativ kann das Administratorkonto auch die Zuordnung Ihres Kontos zu seiner Organisation aufheben und es daraus entfernen.

Konten, die per Einladung verknüpft sind, haben dieselbe allgemeine account-to-member Administratorbeziehung wie Konten, die von verknüpft sind AWS Organizations, wie unter beschriebenGrundlegendes zur Beziehung zwischen GuardDuty Administratorkonto und Mitgliedskonten. Benutzer mit Administratorkonten für Einladungen können jedoch nicht GuardDuty im Namen der zugehörigen Mitgliedskonten aktivieren oder andere Konten innerhalb ihrer AWS Organizations Organisation einsehen, die keine Mitglieder sind.

> **Important**
>
> Bei der Erstellung von Mitgliedskonten mit dieser Methode kann es GuardDuty zu einer überregionalen Datenübertragung kommen. GuardDuty verwendet zur Überprüfung der E-Mail-Adressen von Mitgliedskonten einen E-Mail-Bestätigungsdienst, der nur in der Region USA Ost (Nord-Virginia) verfügbar ist.

Hinzufügen und verwalten von Konten auf Einladung

Wählen Sie eine der Zugriffsmethoden, um Konten hinzuzufügen und einzuladen, GuardDuty Mitgliedskonten als GuardDuty Administratorkonto zu werden.

Console

Schritt 1: Konto hinzufügen

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Wählen Sie im oberen Bereich Konten auf Einladung hinzufügen aus.
4. Geben Sie auf der Seite Mitgliedskonten hinzufügen unter Kontodetails eingeben die AWS-Konto ID und E-Mail-Adresse ein, die mit dem Konto verknüpft sind, das Sie hinzufügen möchten.
5. Um eine weitere Zeile hinzuzufügen, in der die Kontodetails nacheinander eingegeben werden können, wählen Sie Weiteres Konto hinzufügen. Sie können auch CSV-Datei mit Kontodetails hochladen wählen, um mehrere Konten gleichzeitig hinzuzufügen.

> **Important**
>
> Die erste Zeile Ihrer CSV-Datei muss wie im folgenden Beispiel den folgenden Header enthalten – `Account ID,Email`. Jede nachfolgende Zeile muss eine einzige gültige AWS-Konto ID und die zugehörige E-Mail-Adresse enthalten. Das Format einer Zeile ist gültig, wenn sie nur eine AWS-Konto ID und die zugehörige E-Mail-Adresse enthält, die durch ein Komma getrennt sind.
>
> ```
> Account ID,Email
> 555555555555,user@example.com
> ```

6. Nachdem Sie alle Kontodetails hinzugefügt haben, wählen Sie Weiter. Sie können die neu hinzugefügten Konten in der Tabelle Konten einsehen. Der Status dieser Konten lautet Einladung nicht gesendet. Informationen zum Senden einer Einladung an ein oder mehrere hinzugefügte Konten finden Sie unter Step 2 - Invite an account.

Schritt 2: Ein Konto einladen

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Wählen Sie ein oder mehrere Konten aus, die Sie zu Amazon einladen möchten GuardDuty.
4. Wählen Sie im Drop-down-Menü Aktionen und dann Einladen aus.
5. Geben Sie im GuardDuty Dialogfeld „Einladung zu“ eine (optionale) Einladungsnachricht ein.

   Wenn das eingeladene Konto nicht über E-Mail-Zugang verfügt, aktivieren Sie das Kontrollkästchen Auch eine E-Mail-Benachrichtigung an den Root-Benutzer auf dem AWS-Konto des Eingeladenen senden und eine Warnmeldung im AWS Health Dashboard des Eingeladenen erzeugen.
6. Wählen Sie Send invitation (Einladung senden) aus. Wenn die eingeladenen Personen Zugriff auf die angegebene E-Mail-Adresse haben, können sie sich die Einladung ansehen, indem sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/ öffnen.
7. Wenn ein Eingeladener die Einladung annimmt, ändert sich der Wert in der Spalte Status in Eingeladen. Weitere Informationen zur Annahme einer Einladung finden Sie unter Step 3 - Accept an invitation.

Schritt 3: Eine Einladung annehmen

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   > **Important**
   >
   > Sie müssen sie aktivieren, GuardDuty bevor Sie eine Mitgliedschaftseinladung ansehen oder annehmen können.

2. Gehen Sie nur dann wie folgt vor, wenn Sie es GuardDuty noch nicht aktiviert haben. Andernfalls können Sie diesen Schritt überspringen und mit dem nächsten Schritt fortfahren.

   Wenn Sie es noch nicht aktiviert haben GuardDuty, wählen Sie auf der GuardDuty Amazon-Seite Erste Schritte aus.

   Wählen Sie auf der GuardDuty Seite Willkommen bei die Option Aktivieren aus GuardDuty.
3. Gehen Sie nach der Aktivierung GuardDuty für Ihr Konto wie folgt vor, um die Einladung zur Mitgliedschaft anzunehmen:

   a. Wählen Sie im Navigationsbereich Settings (Einstellungen).
   b. Wählen Sie -Accounts (Konten).
   c. Stellen Sie sicher, dass Sie bei den Konten den Inhaber des Kontos verifizieren, von dem Sie die Einladung annehmen. Aktivieren Sie Annehmen, um die Einladung zur Mitgliedschaft anzunehmen.
4. Nachdem Sie die Einladung angenommen haben, wird Ihr Konto zu einem GuardDuty Mitgliedskonto. Das Konto, dessen Besitzer die Einladung gesendet hat, wird zum GuardDuty Administratorkonto. Das Administratorkonto wird wissen, dass Sie die Einladung angenommen haben. Die Kontentabelle in ihrem GuardDuty Konto wird aktualisiert.
   Der Wert in der Spalte Status, der Ihrer Mitgliedskonto-ID entspricht, wird auf Aktiviert geändert. Der Inhaber des Administratorkontos kann nun die Konfigurationen GuardDuty und Schutzpläne für Ihr Konto einsehen und verwalten. Das Administratorkonto kann auch die für Ihr Mitgliedskonto generierten GuardDuty Ergebnisse einsehen und verwalten.

API/CLI

Sie können über die API-Operationen ein GuardDuty Administratorkonto festlegen und GuardDuty Mitgliedskonten auf Einladung erstellen oder hinzufügen. Führen Sie die folgenden GuardDuty API-Operationen aus, um Administratorkonten und Mitgliedskonten in festzulegen. GuardDuty

Führen Sie das folgende Verfahren mit den Anmeldeinformationen des Kontos aus AWS-Konto , das Sie als GuardDuty Administratorkonto festlegen möchten.

Mitgliedskonten erstellen oder hinzufügen

1. Führen Sie den CreateMembersAPI-Vorgang mit den Anmeldeinformationen des AWS Kontos aus, das GuardDuty aktiviert wurde. Dies ist das Konto, das Sie als GuardDuty Administratorkonto verwenden möchten.

   Sie müssen die Melder-ID des AWS Girokontos sowie die Konto-ID und E-Mail-Adresse der Konten angeben, denen Sie GuardDuty beitreten möchten. Sie können mit dieser API-Operation ein oder mehrere Mitglieder erstellen.

   Sie können auch die AWS Befehlszeilentools verwenden, um ein Administratorkonto festzulegen, indem Sie den folgenden CLI-Befehl ausführen. Stellen Sie sicher, dass Sie Ihre eigene gültige Detektor-ID, Konto-ID und E-Mail verwenden.

   Das `detectorId` für Ihr Konto und Ihre aktuelle Region gültige Adresse finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

   ```
   aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   account-details AccountId=111122223333,Email=guardduty-member@organization.com
   ```

2. Verwenden Sie für die Ausführung InviteMembersdie Anmeldeinformationen des AWS Kontos, das GuardDuty aktiviert wurde. Dies ist das Konto, das Sie als GuardDuty Administratorkonto verwenden möchten.

   Sie müssen die Melder-ID des AWS Girokontos und die Konto-IDs der Konten angeben, denen Sie GuardDuty beitreten möchten. Sie können mit dieser API-Operation ein oder mehrere Mitglieder einladen.

   > **Note**
   >
   > Sie können mit dem `message`-Anfrageparameter auch eine optionale Einladungsbenachrichtigung erstellen.

   Sie können sie auch verwenden AWS Command Line Interface , um Mitgliedskonten festzulegen, indem Sie den folgenden Befehl ausführen. Stellen Sie sicher, dass Sie Ihre

eigene gültige Detektor-ID sowie gültige Konto-IDs für die Konten verwenden, die Sie einladen möchten.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 111122223333
```

Einladungen annehmen

Führen Sie das folgende Verfahren mit den Anmeldeinformationen der einzelnen AWS Konten aus, die Sie als GuardDuty Mitgliedskonto festlegen möchten.

1. Führen Sie den CreateDetectorAPI-Vorgang für jedes AWS Konto aus, das als GuardDuty Mitgliedskonto eingeladen wurde und das Sie annehmen möchten.

   Sie müssen angeben, ob die Detektorressource mithilfe des GuardDuty Dienstes aktiviert werden soll. Ein Detektor muss erstellt und aktiviert werden, damit er GuardDuty betriebsbereit ist. Sie müssen die Aktivierung zuerst aktivieren, GuardDuty bevor Sie eine Einladung annehmen können.

   Sie können dies auch mithilfe der AWS Befehlszeilentools mit dem folgenden CLI-Befehl tun.

   ```
   aws guardduty create-detector --enable
   ```

2. Führen Sie den AcceptAdministratorInvitationAPI-Vorgang für jedes AWS Konto aus, für das Sie die Einladung zur Mitgliedschaft annehmen möchten, und verwenden Sie dabei die Anmeldeinformationen dieses Kontos.

   Sie müssen die Melder-ID dieses AWS Kontos für das Mitgliedskonto, die Konto-ID des Administratorkontos, das die Einladung gesendet hat, und die Einladungs-ID der Einladung, die Sie annehmen, angeben. Die Konto-ID des Administratorkontos finden Sie in der Einladungs-E-Mail. Sie können sie auch mittels des API-Vorgangs ListInvitations ermitteln.

   Sie können eine Einladung auch mit den AWS Befehlszeilentools annehmen, indem Sie den folgenden CLI-Befehl ausführen. Stellen Sie sicher, dass Sie eine gültige Detektor-ID, Administratorkonto-ID und Einladungs-ID verwenden.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ - Konsole.

```
aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --administrator-id 444455556666 --invitation-
id 84b097800250d17d1872b34c4daadcf5
```

Konsolidierung von GuardDuty Administratorkonten unter einem einzigen delegierten GuardDuty Administratorkonto der Organisation

GuardDuty empfiehlt die Verwendung von Assoziation bis AWS Organizations zur Verwaltung von Mitgliedskonten unter einem delegierten GuardDuty Administratorkonto. Sie können das unten beschriebene Beispielverfahren verwenden, um das Administratorkonto und das per Einladung zugeordnete Mitglied in einer Organisation unter einem einzigen GuardDuty delegierten GuardDuty Administratorkonto zu konsolidieren.

> **Note**
>
> Konten, die bereits von einem delegierten GuardDuty Administratorkonto verwaltet werden, oder aktive Mitgliedskonten, die einem delegierten GuardDuty Administratorkonto zugeordnet sind, können keinem anderen delegierten GuardDuty Administratorkonto hinzugefügt werden. Jede Organisation kann nur über ein delegiertes GuardDuty Administratorkonto pro Region verfügen, und jedes Mitgliedskonto kann nur über ein delegiertes Administratorkonto verfügen. GuardDuty

Wählen Sie eine der Zugriffsmethoden, um GuardDuty Administratorkonten unter einem einzigen delegierten GuardDuty Administratorkonto zu konsolidieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Verwenden Sie die Anmeldeinformationen des Verwaltungskontos der Organisation, um sich anzumelden.

2. Alle Konten, die Sie verwalten möchten, GuardDuty müssen Teil Ihrer Organisation sein. Informationen zum Hinzufügen eines Kontos zu Ihrer Organisation finden Sie unter Einen AWS-Konto einladen, Ihrer Organisation beizutreten.
3. Stellen Sie sicher, dass alle Mitgliedskonten dem Konto zugeordnet sind, das Sie als einziges delegiertes GuardDuty Administratorkonto festlegen möchten. Trennen Sie alle Mitgliedskonten, die noch mit den bereits vorhandenen Administratorkonten verknüpft sind.

   Die folgenden Schritte helfen Ihnen dabei, Mitgliedskonten vom bereits vorhandenen Administratorkonto zu trennen:

   a. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
   b. Um sich anzumelden, verwenden Sie die Anmeldeinformationen des bereits vorhandenen Administratorkontos.
   c. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
   d. Wählen Sie auf der Seite Konten ein oder mehrere Konten aus, die Sie vom Administratorkonto trennen möchten.
   e. Wählen Sie Aktionen und dann Konto trennen.
   f. Wählen Sie Bestätigen, um den Schritt abzuschließen.
4. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Verwenden Sie die Anmeldeinformationen des Verwaltungskontos, um sich anzumelden.
5. Wählen Sie im Navigationsbereich Settings (Einstellungen). Geben Sie auf der Seite Einstellungen das delegierte GuardDuty Administratorkonto für die Organisation an.
6. Melden Sie sich mit dem angegebenen delegierten Administratorkonto an. GuardDuty
7. Fügen Sie Mitglieder der Organisation hinzu. Weitere Informationen finden Sie unter GuardDuty Konten verwalten mit AWS Organizations.

API/CLI

1. Alle Konten, die Sie verwalten möchten, GuardDuty müssen Teil Ihrer Organisation sein. Informationen zum Hinzufügen eines Kontos zu Ihrer Organisation finden Sie unter Einen AWS-Konto einladen, Ihrer Organisation beizutreten.
2. Stellen Sie sicher, dass alle Mitgliedskonten dem Konto zugeordnet sind, das Sie als einziges delegiertes GuardDuty Administratorkonto festlegen möchten.

a. Führen Sie DisassociateMembersden Befehl aus, um die Zuordnung aller Mitgliedskonten aufzuheben, die noch mit den bereits vorhandenen Administratorkonten verknüpft sind.

b. Alternativ können Sie den folgenden Befehl ausführen und *777777777777* durch die Melder-ID des bereits vorhandenen Administratorkontos ersetzen, von dem Sie die Verknüpfung mit dem Mitgliedskonto trennen möchten. AWS Command Line Interface Ersetzen Sie *666666666666* durch die AWS-Konto -ID des Mitgliedskontos, das Sie trennen möchten.

```
aws guardduty disassociate-members --detector-id 777777777777 --account-
ids 666666666666
```

3. Führen Sie den Befehl aus EnableOrganizationAdminAccount, um ein als delegiertes Administratorkonto zu delegieren. AWS-Konto GuardDuty

   Alternativ können Sie den folgenden Befehl ausführen AWS Command Line Interface , um ein delegiertes Administratorkonto zu delegieren: GuardDuty

```
aws guardduty enable-organization-admin-account --admin-account-id 777777777777
```

4. Fügen Sie Mitglieder der Organisation hinzu. Weitere Informationen finden Sie unter Create or add member member accounts using API.

> **Important**
>
> Um die Effektivität eines GuardDuty regionalen Dienstes zu maximieren, empfehlen wir Ihnen, Ihr delegiertes GuardDuty Administratorkonto festzulegen und alle Mitgliedskonten in jeder Region hinzuzufügen.

GuardDuty In mehreren Konten gleichzeitig aktivieren

Verwenden Sie die folgende Methode, um die Aktivierung GuardDuty in mehreren Konten gleichzeitig durchzuführen.

Verwenden Sie Python-Skripte, um sie GuardDuty in mehreren Konten gleichzeitig zu aktivieren

Sie können die Aktivierung oder Deaktivierung von GuardDuty für mehrere Konten automatisieren, indem Sie die Skripts aus dem Beispiel-Repository bei Amazon GuardDuty Multiaccount Scripts verwenden. Gehen Sie wie in diesem Abschnitt beschrieben vor, GuardDuty um eine Liste von Mitgliedskonten zu aktivieren, die Amazon EC2 verwenden. Informationen zur Verwendung des Deaktivierungsskripts oder zur lokalen Einrichtung des Skripts finden Sie in den Anweisungen im geteilten Link.

Das `enableguardduty.py` Skript aktiviert GuardDuty, sendet Einladungen vom Administratorkonto aus und akzeptiert Einladungen in allen Mitgliedskonten. Das Ergebnis ist ein GuardDuty Administratorkonto, das alle Sicherheitsergebnisse für alle Mitgliedskonten enthält. Da GuardDuty es nach Regionen isoliert ist, werden die Ergebnisse für jedes Mitgliedskonto auf die entsprechende Region im Administratorkonto übertragen. Beispielsweise enthält die Region us-east-1 in Ihrem GuardDuty Administratorkonto die Sicherheitsergebnisse für alle us-east-1-Ergebnisse aller zugehörigen Mitgliedskonten.

Diese Skripte haben eine Abhängigkeit von einer gemeinsam genutzten IAM-Rolle mit der verwalteten Richtlinie – AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess. Diese Richtlinie gewährt Entitäten Zugriff auf das Administratorkonto GuardDuty und muss in jedem Konto, für das Sie die Aktivierung aktivieren möchten, vorhanden sein GuardDuty.

Der folgende Prozess ist standardmäßig GuardDuty in allen verfügbaren Regionen aktiviert. Sie können die Aktivierung nur GuardDuty in bestimmten Regionen durchführen, indem Sie das optionale `--enabled_regions` Argument verwenden und eine durch Kommas getrennte Liste von Regionen angeben. Sie können die Einladungsnachricht, die an Mitgliedskonten gesendet wird, optional auch anpassen, indem Sie `enableguardduty.py` öffnen und die Zeichenfolge `gd_invite_message` bearbeiten.

1. Erstellen Sie eine IAM-Rolle im GuardDuty Administratorkonto und fügen Sie die zu aktivierende AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess Richtlinie an. GuardDuty
2. Erstellen Sie eine IAM-Rolle für jedes Mitgliedskonto, das Sie von Ihrem GuardDuty Administratorkonto verwalten möchten. Diese Rolle muss denselben Namen haben wie die in Schritt 1 erstellte Rolle, sie sollte das Administratorkonto als vertrauenswürdige Entität zulassen und sie sollte dieselbe AmazonGuardDutyFullAccess verwaltete Richtlinie haben, die zuvor beschrieben wurde.

3. Starten Sie eine neue Amazon Linux-Instance mit einer zugeordneten Rolle mit der folgenden Vertrauensstellung, die es der Instance ermöglicht, eine Servicerolle anzunehmen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Melden Sie sich bei der neuen Instance an und führen Sie die folgenden Befehle aus, um sie einzurichten.

```
sudo yum install git python
sudo yum install python-pip
pip install boto3
aws configure
git clone https://github.com/aws-samples/amazon-guardduty-multiaccount-scripts.git
cd amazon-guardduty-multiaccount-scripts
sudo chmod +x disableguardduty.py enableguardduty.py
```

5. Erstellen Sie eine CSV-Datei mit einer Liste von Konto-IDs und E-Mails der Mitgliedskonten, denen Sie in Schritt 2 eine Rolle hinzugefügt haben. Konten müssen eines pro Zeile angezeigt werden, und die Konto-ID und die E-Mail-Adresse müssen wie im folgenden Beispiel durch ein Komma voneinander getrennt sein.

```
111122223333,guardduty-member@organization.com
```

> **Note**
>
> Die CSV-Datei muss sich am selben Speicherort wie das Skript `enableguardduty.py` befinden. Sie können eine vorhandene CSV-Datei mit der folgenden Methode aus Amazon S3 in Ihr aktuelles Verzeichnis kopieren.

```
aws s3 cp s3://my-bucket/my_key_name example.csv
```

6. Führen Sie das Python-Skript aus. Stellen Sie sicher, dass Sie Ihre GuardDuty Administratorkonto-ID, den Namen der in den ersten Schritten erstellten Rolle und den Namen Ihrer CSV-Datei als Argumente angeben.

```
python enableguardduty.py --master_account 444455556666 --assume_role
 roleName accountID.csv
```

Schätzung der Kosten GuardDuty

Sie können die GuardDuty Konsolen- oder API-Operationen verwenden, um die täglichen durchschnittlichen Nutzungskosten für GuardDuty zu schätzen. Während der 30-tägigen kostenlosen Testphase geht die Kostenschätzung davon aus, wie hoch Ihre geschätzten Kosten nach dem Testzeitraum sein werden. Wenn Sie in einer Umgebung mit mehreren Konten arbeiten, kann Ihr GuardDuty Administratorkonto die Kostenkennzahlen für alle Mitgliedskonten überwachen.

Sie können die Kostenschätzung anhand der folgenden Metriken einsehen:

- Konto-ID — Listet die geschätzten Kosten für Ihr Konto oder für Ihre Mitgliedskonten auf, wenn Sie als GuardDuty Administratorkonto arbeiten.
- Datenquelle — Listet die geschätzten Kosten für die angegebene Datenquelle für die folgenden GuardDuty Datenquellentypen auf: VPC-Flussprotokolle, CloudTrail Verwaltungsprotokolle, CloudTrail Datenereignisse oder DNS-Protokolle.
- Funktionen — Listet die geschätzten Kosten für die angegebene Datenquelle für die folgenden GuardDuty Funktionen auf: CloudTrail Datenereignisse für S3, EKS Audit Log Monitoring, EBS-Volumendaten, RDS-Anmeldeaktivität, EKS Runtime Monitoring, Fargate Runtime Monitoring, EC2 Runtime Monitoring oder Lambda Network Activity Monitoring.
- S3-Buckets – Listet die geschätzten Kosten für S3-Datenereignisse in einem bestimmten Bucket oder die teuersten Buckets für Konten in Ihrer Umgebung auf.

> **Note**
>
> S3-Bucket-Statistiken sind nur verfügbar, wenn S3 Protection für das Konto aktiviert ist. Weitere Informationen finden Sie unter Amazon S3 S3-Schutz bei Amazon GuardDuty.

Verstehen Sie, wie die Nutzungskosten berechnet werden GuardDuty

Die in der GuardDuty Konsole angezeigten Schätzungen können geringfügig von denen auf Ihrer AWS Billing and Cost Management Konsole abweichen. In der folgenden Liste wird erläutert, wie die Nutzungskosten GuardDuty geschätzt werden:

- Die geschätzte GuardDuty Nutzung bezieht sich nur auf die aktuelle Region.

- Die GuardDuty Nutzungskosten basieren auf den Nutzungsdaten der letzten 30 Tage.
- Die Kostenschätzung für die Nutzung der Testversion beinhaltet die Schätzung für grundlegende Datenquellen und Feature, die sich derzeit im Testzeitraum befinden. Für jede Funktion und Datenquelle GuardDuty gibt es einen eigenen Testzeitraum, der sich jedoch mit dem Testzeitraum von GuardDuty oder einer anderen Funktion, die gleichzeitig aktiviert wurde, überschneiden kann.
- Die geschätzte GuardDuty Nutzung beinhaltet GuardDuty Mengenrabatte pro Region, wie auf der GuardDuty Amazon-Preisseite detailliert beschrieben, jedoch nur für einzelne Konten, die den Volumenpreisstufen entsprechen. Mengenrabatte sind in den Schätzungen für die kombinierte Gesamtnutzung zwischen Konten innerhalb einer Organisation nicht enthalten. Informationen zu Mengenrabatten bei kombinierter Nutzung finden Sie unter AWS -Abrechnung: Mengenrabatte.
- Die Summe der Nutzungskosten für die einzelnen AWS-Konto Benutzer in Ihrer Organisation entspricht möglicherweise nicht immer den geschätzten Kosten der letzten 30 Tage für die ausgewählte Datenquelle. Die Preisstufe kann sich ändern, wenn mehr Ereignisse oder Daten GuardDuty verarbeitet werden. Weitere Informationen finden Sie unter Preisstufen im AWS Billing Benutzerhandbuch.

Laufzeitüberwachung — Wie sich VPC-Flow-Logs von EC2-Instances auf die Nutzungskosten auswirken

Wenn Sie den Security Agent (entweder manuell oder über GuardDuty) in EKS Runtime Monitoring oder Runtime Monitoring for EC2-Instances verwalten und derzeit auf einer Amazon EC2 EC2-Instance bereitgestellt GuardDuty ist und diese Gesammelte Laufzeit-Ereignistypen von dieser Instance empfängt, GuardDuty wird Ihnen die Analyse der VPC-Flow-Logs von dieser Amazon EC2 EC2-Instance nicht in Rechnung gestellt. AWS-Konto Dadurch werden doppelte Nutzungskosten für das Konto GuardDuty vermieden.

Wie GuardDuty schätzt man die Nutzungskosten für CloudTrail Veranstaltungen

Wenn Sie diese Option aktivieren GuardDuty, werden automatisch AWS CloudTrail Ereignisprotokolle verwendet, die für Ihr Konto im ausgewählten Bereich aufgezeichnet wurden AWS-Region. GuardDuty repliziert globale Service-Ereignisprotokolle und verarbeitet diese Ereignisse dann unabhängig voneinander in jeder Region, in der Sie sie GuardDuty aktiviert haben. Dies hilft bei der GuardDuty Verwaltung von Benutzer- und Rollenprofilen in jeder Region, um Anomalien zu identifizieren.

Ihre CloudTrail Konfiguration hat keinen Einfluss auf die GuardDuty Nutzungskosten oder die Art und Weise, wie Ihre GuardDuty Ereignisprotokolle verarbeitet werden. Ihre GuardDuty Nutzungskosten hängen von der Nutzung der AWS APIs ab, bei denen Sie sich anmelden CloudTrail. Weitere Informationen finden Sie unter AWS CloudTrail Ereignisprotokolle.

Überprüfung der GuardDuty Nutzungsstatistiken

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die Nutzungsstatistiken für Ihr GuardDuty Konto zu überprüfen. Wenn Sie ein GuardDuty Administratorkonto haben, helfen Ihnen die folgenden Methoden dabei, die Nutzungsstatistiken für alle Mitglieder zu überprüfen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie das GuardDuty Administratorkonto verwenden.
2. Wählen Sie im Navigationsbereich Benutzer.
3. Auf der Seite Nutzung kann ein GuardDuty Administratorkonto mit Mitgliedskonten die geschätzten Organisationskosten der letzten 30 Tage einsehen. Dies sind die geschätzten Gesamtnutzungskosten für Ihre Organisation.
4. GuardDuty Administratorkonten mit Mitgliedern können entweder die Aufschlüsselung der Nutzungskosten nach Datenquelle oder nach Konten einsehen. Einzelne oder eigenständige Konten können die Aufschlüsselung nach Datenquelle einsehen.

   Wenn Sie Mitgliedskonten haben, können Sie die Statistiken für ein einzelnes Konto einsehen, indem Sie dieses Konto in der Tabelle Konten auswählen.

   Wenn Sie auf der Registerkarte Nach Datenquellen eine Datenquelle auswählen, der Nutzungskosten zugeordnet sind, ist die entsprechende Summe der Kostenaufschlüsselung auf Kontoebene möglicherweise nicht immer dieselbe.

API/CLI

Führen Sie den GetUsageStatisticsAPI-Vorgang mit den Anmeldeinformationen des GuardDuty Administratorkontos aus. Geben Sie die folgenden Informationen ein, um den Befehl auszuführen:

- (Erforderlich) Geben Sie die regionale GuardDuty Melder-ID des Kontos an, für das Sie die Statistiken abrufen möchten.

- (Erforderlich) Geben Sie eine der folgenden Arten von Statistiken an, die abgerufen werden sollen: `SUM_BY_ACCOUNT | SUM_BY_DATA_SOURCE | SUM_BY_RESOURCE | SUM_BY_FEATURE | TOP_ACCOUNTS_BY_FEATURE`.

  Unterstützt derzeit `TOP_ACCOUNTS_BY_FEATURE` nicht das Abrufen von Nutzungsstatistiken für`RDS_LOGIN_EVENTS`.
- (Erforderlich) Stellen Sie eine oder mehrere Datenquellen oder Funktionen zur Abfrage Ihrer Nutzungsstatistiken bereit.
- (Optional) Geben Sie eine Liste mit Konto-IDs an, für die Sie Nutzungsstatistiken abrufen möchten.

Sie können auch die AWS Command Line Interface verwenden. Der folgende Befehl ist ein Beispiel für das Abrufen der Nutzungsstatistiken für alle Datenquellen und Funktionen, berechnet nach Konten. Stellen Sie sicher, dass Sie die `detector-id` durch Ihre eigene gültige Detektor-ID ersetzen. Bei eigenständigen Konten gibt dieser Befehl die Nutzungskosten der letzten 30 Tage nur für Ihr Konto zurück. Wenn Sie ein GuardDuty Administratorkonto mit Mitgliedskonten haben, werden die Kosten für alle Mitglieder nach Konten aufgelistet.

Die Angaben `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/ -Konsole.

Ersetzen Sie es `SUM_BY_ACCOUNT` durch den Typ, mit dem Sie die Nutzungsstatistiken berechnen möchten.

Um nur die Kosten für Datenquellen zu überwachen

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"DataSources":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_LOGS", "KUBERNETES_AUDIT_LOGS",
 "EC2_MALWARE_SCAN"]}'
```

Um die Kosten für Funktionen zu überwachen

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"Features":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_DATA_EVENTS", "EKS_AUDIT_LOGS",
 "EBS_MALWARE_PROTECTION", "RDS_LOGIN_EVENTS", "LAMBDA_NETWORK_LOGS",
 "EKS_RUNTIME_MONITORING", "FARGATE_RUNTIME_MONITORING", "EC2_RUNTIME_MONITORING"]}'
```

Sicherheit in Amazon GuardDuty

Die Sicherheit in der Cloud hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das Modell der geteilten Verantwortlichkeit beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud selbst – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Informationen zu den Compliance-Programmen, die für GuardDuty gelten, finden Sie unter Im Rahmen des Compliance-Programms gültige AWS-Services.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, einschließlich der Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der geteilten Verantwortung bei der Verwendung von GuardDuty einsetzen können. Es zeigt Ihnen, wie Sie GuardDuty konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren außerdem, wie Sie andere AWS-Services verwenden, um Ihre GuardDuty-Ressourcen zu überwachen und zu schützen.

Inhalt

Datenschutz bei Amazon GuardDuty

Das AWS Modell der gilt für den Datenschutz bei Amazon GuardDuty. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole, der API GuardDuty oder den SDKs arbeiten oder diese anderweitig AWS-Services verwenden. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine

Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Verschlüsselung im Ruhezustand

Alle GuardDuty Kundendaten werden im Ruhezustand mithilfe von AWS Verschlüsselungslösungen verschlüsselt.

GuardDuty Daten, wie z. B. Ergebnisse, werden im Ruhezustand mithilfe von AWS Key Management Service (AWS KMS) unter Verwendung von eigenen, vom AWS Kunden verwalteten Schlüsseln verschlüsselt.

Verschlüsselung während der Übertragung

GuardDuty analysiert Protokolldaten von anderen Diensten. GuardDuty verschlüsselt alle Daten während der Übertragung von diesen Services mit HTTPS und KMS. Sobald die benötigten Informationen aus den Protokollen GuardDuty extrahiert wurden, werden sie verworfen. Weitere Informationen darüber, wie Informationen aus anderen Diensten GuardDuty verwendet werden, finden Sie unter GuardDuty Datenquellen.

GuardDuty Daten werden bei der Übertragung zwischen Diensten verschlüsselt.

Abmeldung von der Verwendung Ihrer Daten zur Serviceverbesserung

Sie können sich dafür entscheiden, die Verwendung Ihrer Daten zur Entwicklung GuardDuty und Verbesserung anderer AWS Sicherheitsdienste abzulehnen, indem Sie die AWS Organizations Opt-Out-Richtlinie verwenden. Sie können sich dafür entscheiden, sich abzumelden, auch wenn derzeit GuardDuty keine derartigen Daten erfasst werden. Weitere Informationen zur Deaktivierung finden Sie in den Opt-Out-Richtlinien für KI-Services im Benutzerhandbuch für AWS Organizations .

> **Note**
>
> Damit Sie die Opt-Out-Richtlinie nutzen können, müssen Ihre AWS Konten zentral von verwaltet werden AWS Organizations. Wenn Sie noch keine Organisation für Ihre AWS Konten erstellt haben, finden Sie weitere Informationen unter Organisation erstellen und verwalten im AWS Organizations Benutzerhandbuch.

Opt-Out hat folgende Auswirkungen:

- GuardDuty löscht die Daten, die es vor Ihrer Abmeldung gesammelt und gespeichert hat, um den Service zu verbessern (falls vorhanden).
- Nach Ihrer Abmeldung GuardDuty werden diese Daten nicht mehr zu Zwecken der Serviceverbesserung gesammelt oder gespeichert.

In den folgenden Themen wird erklärt, wie die einzelnen Funktionen GuardDuty möglicherweise Ihre Daten zur Serviceverbesserung verarbeiten.

Inhalt

GuardDuty Überwachung der Laufzeit

GuardDuty Runtime Monitoring bietet Runtime-Bedrohungserkennung für Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster, nur AWS Fargate (Fargate) Amazon Elastic Container Service (Amazon ECS) und Amazon Elastic Compute Cloud (Amazon EC2) -Instances in Ihrer Umgebung. AWS Nachdem Sie Runtime Monitoring aktiviert und den GuardDuty Security Agent für Ihre Ressource bereitgestellt haben, GuardDuty beginnt es mit der Überwachung und Analyse der mit Ihrer Ressource verknüpften Runtime-Ereignisse. Zu diesen Runtime-Ereignistypen gehören Prozessereignisse, Container-Ereignisse, DNS-Ereignisse und mehr. Weitere Informationen finden Sie unter Gesammelte Runtime-Ereignistypen, die verwendet GuardDuty .

Obwohl GuardDuty jetzt Befehlszeilenargumente gesammelt werden, die Sie an Ihre Workloads weiterleiten können, werden diese Argumente derzeit nicht zur Serviceverbesserung verwendet (dies könnte in future der Fall sein). In Erwartung neuer Regeln und Erkenntnisse zur Bedrohungserkennung, die bald veröffentlicht werden, haben wir damit begonnen, Befehlszeilenargumente zu sammeln. Ihr Vertrauen, Ihre Privatsphäre und die Sicherheit Ihrer Inhalte haben für uns höchste Priorität und wir stellen sicher, dass unsere Nutzung unseren Verpflichtungen Ihnen gegenüber entspricht. Weitere Informationen finden Sie unter Häufig gestellte Fragen zum Datenschutz.

GuardDuty Schutz vor Schadsoftware

GuardDuty Malware Protection scannt und erkennt Malware, die in EBS-Volumes enthalten ist, die an Ihre potenziell gefährdeten Amazon EC2 EC2-Instance- und Container-Workloads angehängt sind. Wenn GuardDuty Malware Protection eine EBS-Volume-Datei als bösartig oder schädlich

identifiziert, sammelt und speichert GuardDuty Malware Protection diese Datei, um die Malware-Erkennungen und den Service weiterzuentwickeln und zu verbessern. GuardDuty Diese Datei kann auch zur Entwicklung und Verbesserung anderer AWS Sicherheitsdienste verwendet werden. Ihr Vertrauen, Ihre Privatsphäre und die Sicherheit Ihrer Inhalte haben für uns höchste Priorität und wir stellen sicher, dass unsere Nutzung unseren Verpflichtungen Ihnen gegenüber entspricht. Weitere Informationen finden Sie unter Häufig gestellte Fragen zum Datenschutz.

Protokollierung Amazon GuardDuty Amazon-API-Aufrufen mit AWS CloudTrail

Amazon GuardDuty ist in einen Service integriertAWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Service in ausgeführt wurden GuardDuty. CloudTrail erfasst alle API-Aufrufe GuardDuty als Ereignisse, einschließlich Aufrufe von der GuardDuty Konsole und von Codeaufrufen an die GuardDuty APIs. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon Simple Storage Service (Amazon S3) -Bucket aktivieren, einschließlich Ereignissen für GuardDuty. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, an die die Anfrage gestellt wurde GuardDuty, die IP-Adresse, von der die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen dazu CloudTrail, einschließlich der Konfiguration und Aktivierung, finden Sie im AWS CloudTrailBenutzerhandbuch.

GuardDuty Informationen in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn unterstützte Ereignisaktivitäten in auftreten GuardDuty, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im CloudTrail Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für GuardDuty, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-

Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- In CloudTrail unterstützte Services und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Anmeldeinformationen des Root-Benutzers oder des IAM-Benutzers gestellt wurde
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde
- Ob die Anforderung von einem anderen AWS-Service getätigt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

GuardDuty Ereignisse auf der Kontrollebene in CloudTrail

Standardmäßig CloudTrail protokolliert es alle GuardDuty API-Operationen, die in der Amazon GuardDuty API-Referenz bereitgestellt werden, als Ereignisse in CloudTrail Dateien.

GuardDuty Datenereignisse in CloudTrail

GuardDuty Überwachung der Laufzeitverwendet einen GuardDuty Sicherheitsagenten, der auf Ihren Amazon Elastic Kubernetes Service (Amazon EKS) -Clustern, Amazon Elastic Compute Cloud (Amazon EC2) -Instances und AWS Fargate (nur Amazon Elastic Container Service (Amazon ECS)) Aufgaben installiert ist, um Add-on (`aws-guardduty-agent`) zu sammeln, die Gesammelte Laufzeit-Ereignistypen für Ihre AWS Workloads gesammelt werden, und sendet sie dann zur Bedrohungserkennung und GuardDuty -analyse an.

Protokollierung und Überwachung von Datenereignissen

Sie können die AWS CloudTrail Protokolle optional so konfigurieren, dass die Datenereignisse für Ihren Security Agent angezeigt werden. GuardDuty

Informationen zum Erstellen und Konfigurieren CloudTrail finden Sie unter Datenereignisse im AWS CloudTrailBenutzerhandbuch und folgen Sie den Anweisungen zur Protokollierung von Datenereignissen mit erweiterten Ereignisauswahlmöglichkeiten in der AWS Management Console. Wenn Sie den Trail protokollieren, stellen Sie sicher, dass Sie die folgenden Änderungen vornehmen:

- Wählen Sie für den Ereignistyp „Daten“ die Option GuardDuty Detektor aus.
- Wählen Sie für die Protokollauswahlvorlage die Option Alle Ereignisse protokollieren aus.
- Erweitern Sie die JSON-Ansicht für die Konfiguration. Die Ausgabe sollte ähnlich dem folgenden JSON aussehen:

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

Nachdem Sie den Selektor für den Trail aktiviert haben, navigieren Sie zur Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/. Sie können die Datenereignisse aus Ihrem S3-Bucket herunterladen, den Sie bei der Konfiguration der CloudTrail Protokolle ausgewählt haben.

Beispiel: Einträge in GuardDuty Protokolldateien

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der das Ereignis auf der Datenebene demonstriert.


```
{
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "111122223333:aws:ec2-instance:i-123412341234example",
            "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-
instance/i-123412341234example",
            "accountId": "111122223333",
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "111122223333:aws:ec2-instance",
                    "arn": "arn:aws:iam::111122223333:role/aws:ec2-instance",
                    "accountId": "111122223333",
                    "userName": "aws:ec2-instance"
                },
                "attributes": {
                    "creationDate": "2023-03-05T04:00:21Z",
                    "mfaAuthenticated": "false"
                },
                "ec2RoleDelivery": "2.0"
            }
        },
        "eventTime": "2023-03-05T06:03:49Z",
        "eventSource": "guardduty.amazonaws.com",
        "eventName": "SendSecurityTelemetry",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "54.240.230.177",
        "userAgent": "aws-sdk-rust/0.54.1 os/linux lang/rust/1.66.0",
```

```
        "requestParameters": null,
        "responseElements": null,
        "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
        "readOnly": false,
        "resources": [{
            "accountId": "111122223333",
            "type": "AWS::GuardDuty::Detector",
            "ARN": "arn:aws:guardduty:us-
west-2:111122223333:detector/12abc34d567e8fa901bc2d34e56789f0"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "111122223333",
        "eventCategory": "Data",
        "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "guardduty-data.us-east-1.amazonaws.com"
        }
    }
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `CreateIPThreatIntelSet` Aktion demonstriert (Ereignis auf der Steuerungsebene).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-06-14T22:54:20Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
```

```
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2018-06-14T22:57:56Z",
    "eventSource": "guardduty.amazonaws.com",
    "eventName": "CreateThreatIntelSet",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.240.230.177",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "detectorId": "12abc34d567e8fa901bc2d34e56789f0",
        "name": "Example",
        "format": "TXT",
        "activate": false,
        "location": "https://s3.amazonaws.com/bucket.name/file.txt"
    },
    "responseElements": {
        "threatIntelSetId": "1ab200428351c99d859bf61992460d24"
    },
    "requestID": "5f6bf981-7026-11e8-a9fc-5b37d2684c5c",
    "eventID": "81337b11-e5c8-4f91-b141-deb405625bc9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```


Aus diesem Ereignis Informationen können Sie ersehen, dass die Anfrage gestellt wurde, um eine Bedrohungsliste `Example` in GuardDuty zu erstellen. Sie können auch sehen, dass die Anfrage von einem Benutzer namens Alice am 14. Juni 2018 gemacht wurde.

Identity and Access Management für Amazon GuardDuty

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. GuardDuty IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie tätig sind. GuardDuty

Dienstbenutzer — Wenn Sie den GuardDuty Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr GuardDuty Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie in nicht auf eine Funktion zugreifen können GuardDuty, finden Sie weitere Informationen unterFehlerbehebung Amazon GuardDuty Amazon-Identität und -Zugriff.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die GuardDuty Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf GuardDuty. Es ist Ihre Aufgabe, zu bestimmen, auf welche GuardDuty Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM nutzen kann GuardDuty, finden Sie unterSo GuardDuty arbeitet Amazon mit IAM.

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff darauf zu verwalten. GuardDuty Beispiele für GuardDuty identitätsbasierte Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon GuardDuty

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-

Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen, die auf Amazon EC2 ausgeführt werden — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie

mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze

für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.

- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

So GuardDuty arbeitet Amazon mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf verwenden, sollten Sie sich darüber informieren GuardDuty, mit welchen IAM-Funktionen Sie arbeiten können. GuardDuty

IAM-Funktionen, die Sie mit Amazon verwenden können GuardDuty

IAM-Feature	GuardDuty Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie GuardDuty und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für GuardDuty

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für GuardDuty

Beispiele für GuardDuty identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon GuardDuty

Ressourcenbasierte Richtlinien finden Sie in GuardDuty

Unterstützt ressourcenbasierte Richtlinien	Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Richtlinienaktionen für GuardDuty

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der GuardDuty Aktionen finden Sie unter Von Amazon definierte Aktionen GuardDuty in der Service Authorization Reference.

Bei den in der Richtlinie GuardDuty verwendeten Aktionen wird vor der Aktion das folgende Präfix verwendet:

```
guardduty
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "guardduty:action1",
      "guardduty:action2"
         ]
```

Beispiele für GuardDuty identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon GuardDuty

Politische Ressourcen für GuardDuty

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der GuardDuty Ressourcentypen und ihrer ARNs finden Sie unter Von Amazon definierte Ressourcen GuardDuty in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von Amazon definierte Aktionen GuardDuty.

Beispiele für GuardDuty identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon GuardDuty

Bedingungsschlüssel für Richtlinien für GuardDuty

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der GuardDuty Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon GuardDuty in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon definierte Aktionen GuardDuty.

Beispiele für GuardDuty identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon GuardDuty

Zugriffssteuerungslisten (ACLs) in GuardDuty

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Attributbasierte Zugriffskontrolle (ABAC) mit GuardDuty

Unterstützt ABAC (Tags in Richtlinien)	Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Temporäre Anmeldeinformationen verwenden mit GuardDuty

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn

Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Prinzipalberechtigungen für GuardDuty

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für GuardDuty

Unterstützt Servicerollen	Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die GuardDuty Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, GuardDuty wenn Sie dazu eine Anleitung erhalten.

Dienstbezogene Rollen für GuardDuty

Unterstützt serviceverknüpfte Rollen	Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von GuardDuty dienstbezogenen Rollen finden Sie unter. Verwenden von serviceverknüpften Rollen für Amazon GuardDuty

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für Amazon GuardDuty

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Ressourcen zu erstellen oder zu ändern GuardDuty. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von definiert wurden GuardDuty, einschließlich des Formats der ARNs für jeden der Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon GuardDuty in der Service Authorization Reference.

Themen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand GuardDuty Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.

- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der GuardDuty-Konsole

Um auf die GuardDuty Amazon-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Informationen zu den GuardDuty Ressourcen in Ihrem Verzeichnis aufzulisten und einzusehen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die GuardDuty Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die GuardDuty `ConsoleAccess` oder die `ReadOnly` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Erforderliche Berechtigungen zum Aktivieren von GuardDuty

Um Berechtigungen zu gewähren, über die verschiedene IAM-Identitäten (Benutzer, Gruppen und Rollen) verfügen müssen, fügen Sie die erforderliche AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess Richtlinie zur Aktivierung hinzu. GuardDuty

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der OR-API. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
```

```
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Benutzerdefinierte IAM-Richtlinie zur Gewährung von schreibgeschütztem Zugriff auf GuardDuty

Um nur Lesezugriff zu gewähren, können GuardDuty Sie die verwaltete Richtlinie verwenden. `AmazonGuardDutyReadOnlyAccess`

Um eine benutzerdefinierte Richtlinie zu erstellen, die einer IAM-Rolle, einem Benutzer oder einer Gruppe schreibgeschützten Zugriff gewährt GuardDuty, können Sie die folgende Anweisung verwenden:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ListMembers",
                "guardduty:GetMembers",
                "guardduty:ListInvitations",
                "guardduty:ListDetectors",
                "guardduty:GetDetector",
                "guardduty:ListFindings",
                "guardduty:GetFindings",
                "guardduty:ListIPSets",
                "guardduty:GetIPSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:GetThreatIntelSet",
                "guardduty:GetMasterAccount",
                "guardduty:GetInvitationsCount",
                "guardduty:GetFindingsStatistics",
                "guardduty:DescribeMalwareScans",
                "guardduty:UpdateMalwareScanSettings",
                "guardduty:GetMalwareScanSettings"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Zugriff auf Ergebnisse verweigern GuardDuty

Sie können die folgende Richtlinie verwenden, um einer IAM-Rolle, einem Benutzer oder einer Gruppe den Zugriff auf GuardDuty Ergebnisse zu verweigern. Benutzer können keine Ergebnisse oder Details zu Ergebnissen anzeigen, aber sie können auf alle anderen GuardDuty Operationen zugreifen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateDetector",
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "guardduty:CreateIPSet",
                "guardduty:DeleteIPSet",
                "guardduty:UpdateIPSet",
                "guardduty:GetIPSet",
                "guardduty:ListIPSets",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:UpdateThreatIntelSet",
                "guardduty:GetThreatIntelSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:ArchiveFindings",
                "guardduty:UnarchiveFindings",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateMembers",
                "guardduty:InviteMembers",
                "guardduty:GetMembers",
                "guardduty:DeleteMembers",
                "guardduty:DisassociateMembers",
                "guardduty:StartMonitoringMembers",
```

```
                "guardduty:StopMonitoringMembers",
                "guardduty:ListMembers",
                "guardduty:GetMasterAccount",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:AcceptAdministratorInvitation",
                "guardduty:ListInvitations",
                "guardduty:GetInvitationsCount",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteInvitations"
            ],
            "Resource": "*"
        },
         {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

Verwendung einer benutzerdefinierten IAM-Richtlinie zur Beschränkung des Zugriffs auf Ressourcen GuardDuty

Um den Zugriff eines Benutzers auf der GuardDuty Grundlage der Detektor-ID zu definieren, können Sie alle GuardDutyAPI-Aktionen in Ihren benutzerdefinierten IAM-Richtlinien verwenden, mit Ausnahme der folgenden Operationen:

- `guardduty:CreateDetector`
- `guardduty:DeclineInvitations`
- `guardduty:DeleteInvitations`
- `guardduty:GetInvitationsCount`
- `guardduty:ListDetectors`
- `guardduty:ListInvitations`

Verwenden Sie die folgenden Operationen in einer IAM-Richtlinie, um den Zugriff eines Benutzers auf der GuardDuty Grundlage der IPSet-ID und -ID zu definieren: ThreatIntelSet

- `guardduty:DeleteIPSet`
- `guardduty:DeleteThreatIntelSet`
- `guardduty:GetIPSet`
- `guardduty:GetThreatIntelSet`
- `guardduty:UpdateIPSet`
- `guardduty:UpdateThreatIntelSet`

Die folgenden Beispiele zeigen, wie Richtlinien mithilfe einiger der vorhergehenden Vorgänge erstellt werden:

- Diese Richtlinie erlaubt einem Benutzer die Ausführung des `guardduty:UpdateDetector`-Vorgangs mithilfe der Detektor-ID 1234567 in der Region „us-east-1“:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateDetector",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567"
        }
    ]
}
```

- Diese Richtlinie erlaubt einem Benutzer die Ausführung des `guardduty:UpdateIPSet`-Vorgangs mithilfe der Detektor-ID 1234567 und der IPSet-ID 000000 in der Region „us-east-1“:

> **Note**
>
> Stellen Sie sicher, dass der Benutzer über die erforderlichen Berechtigungen für den Zugriff auf vertrauenswürdige IP-Adressen und Bedrohungslisten in verfügt. GuardDuty Weitere Informationen finden Sie unter Erforderliche Berechtigungen für das Hochladen von Listen mit vertrauenswürdigen IPs und Bedrohungslisten.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/000000"
        }
    ]
}
```

- Diese Richtlinie erlaubt einem Benutzer die Ausführung des `guardduty:UpdateIPSet`-Vorgangs mithilfe einer beliebigen Detektor-ID und der IPSet-ID 000000 in der Region „us-east-1“:

> **Note**
>
> Stellen Sie sicher, dass der Benutzer über die erforderlichen Berechtigungen für den Zugriff auf vertrauenswürdige IP-Adressen und Bedrohungslisten in verfügt GuardDuty. Weitere Informationen finden Sie unter Erforderliche Berechtigungen für das Hochladen von Listen mit vertrauenswürdigen IPs und Bedrohungslisten.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
        }
    ]
}
```

- Diese Richtlinie erlaubt einem Benutzer die Ausführung des `guardduty:UpdateIPSet`-Vorgangs mithilfe der Detektor-ID und einer beliebigen IPSet-ID in der Region „us-east-1“:

> **Note**
>
> Stellen Sie sicher, dass der Benutzer über die erforderlichen Berechtigungen für den Zugriff auf vertrauenswürdige IP-Adressen und Bedrohungslisten in verfügt GuardDuty. Weitere Informationen finden Sie unter Erforderliche Berechtigungen für das Hochladen von Listen mit vertrauenswürdigen IPs und Bedrohungslisten.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/*"
        }
    ]
}
```

Verwenden von serviceverknüpften Rollen für Amazon GuardDuty

Amazon GuardDuty verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle (SLR) ist eine einzigartige Art von IAM-Rolle, mit der direkt verknüpft ist. GuardDuty Mit Diensten verknüpfte Rollen sind vordefiniert GuardDuty und enthalten alle Berechtigungen, die GuardDuty erforderlich sind, um andere AWS Dienste in Ihrem Namen aufzurufen.

Mit einer dienstverknüpften Rolle können Sie sie einrichten, GuardDuty ohne die erforderlichen Berechtigungen manuell hinzufügen zu müssen. GuardDuty definiert die Berechtigungen der dienstbezogenen Rolle. Sofern die Berechtigungen nicht anders definiert sind, GuardDuty kann Only die Rolle übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

GuardDuty unterstützt die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen diese Funktion verfügbar GuardDuty ist. Weitere Informationen finden Sie unter Regionen und Endpunkte.

Sie können die GuardDuty dienstverknüpfte Rolle erst löschen, nachdem Sie sie zuerst GuardDuty in allen Regionen deaktiviert haben, in denen sie aktiviert ist. Dadurch werden Ihre GuardDuty Ressourcen geschützt, da Sie die Zugriffsberechtigung nicht versehentlich entziehen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM funktionieren im IAM-Benutzerhandbuch. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Mit dem Dienst verknüpfte Rollenberechtigungen für GuardDuty

GuardDuty verwendet die benannte serviceverknüpfte Rolle (SLR). `AWSServiceRoleForAmazonGuardDuty` Die Spiegelreflexkamera ermöglicht GuardDuty die Ausführung der folgenden Aufgaben. Es ermöglicht auch GuardDuty , die abgerufenen Metadaten der EC2-Instance in die Erkenntnisse einzubeziehen, die sich GuardDuty möglicherweise über die potenzielle Bedrohung ergeben. Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonGuardDuty` vertraut dem Service `guardduty.amazonaws.com`, sodass dieser die Rolle annehmen kann.

Die Berechtigungsrichtlinien helfen bei der GuardDuty Ausführung der folgenden Aufgaben:

- Verwenden Sie Amazon EC2 EC2-Aktionen, um Informationen über Ihre EC2-Instances, Images und Netzwerkkomponenten wie VPCs, Subnetze und Transit-Gateways zu verwalten und abzurufen.
- Verwenden Sie AWS Systems Manager Aktionen, um SSM-Verknüpfungen auf Amazon EC2-Instances zu verwalten, wenn Sie GuardDuty Runtime Monitoring mit automatisiertem Agenten für Amazon EC2 aktivieren. Wenn die GuardDuty automatische Agentenkonfiguration deaktiviert ist, werden nur die EC2-Instances GuardDuty berücksichtigt, die über ein Inclusion-Tag (:) verfügen. `GuardDutyManaged` `true`
- Verwenden Sie AWS Organizations Aktionen, um die zugehörigen Konten und die Organisations-ID zu beschreiben.
- Verwenden Sie Amazon-S3-Aktionen, um Informationen über S3-Buckets und Objekte abzurufen.
- Verwenden Sie AWS Lambda Aktionen, um Informationen über Ihre Lambda-Funktionen und -Tags abzurufen.
- Verwenden Sie Amazon-EKS-Aktionen, um Informationen über die EKS-Cluster zu verwalten und abzurufen und Amazon-EKS-Add-Ons auf EKS-Clustern zu verwalten. Die EKS-Aktionen rufen auch die Informationen über die zugehörigen Tags ab. GuardDuty
- Verwenden Sie IAM, um Serviceverknüpfte Rollenberechtigungen für den Malware Protection zu erstellen, nachdem der Malware Protection aktiviert wurde.
- Verwenden Sie Amazon ECS-Aktionen, um Informationen über die Amazon ECS-Cluster zu verwalten und abzurufen, und verwalten Sie die Amazon ECS-Kontoeinstellungen mit`guarddutyActivate`. Die Aktionen im Zusammenhang mit Amazon ECS rufen auch die Informationen über die zugehörigen Tags ab. GuardDuty

Die Rolle ist mit der folgenden AWS -verwalteten Richtlinie namens `AmazonGuardDutyServiceRolePolicy` konfiguriert.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GuardDutyGetDescribeListPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeSubnets",
```

```
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeTransitGatewayAttachments",
                "organizations:ListAccounts",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketTagging",
                "s3:GetAccountPublicAccessBlock",
                "s3:ListAllMyBuckets",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "lambda:GetFunctionConfiguration",
                "lambda:ListTags",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeSecurityGroups",
                "ecs:ListClusters",
                "ecs:DescribeClusters"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GuardDutyCreateSLRPolicy",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                },
```

```
                "StringLike": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.*.guardduty-data",
                        "com.amazonaws.*.guardduty-data-fips"
                    ]
                }
            }
        },
        {
            "Sid": "GuardDutyModifyDeleteVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpoint",
                "ec2:DeleteVpcEndpoints"
            ],
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpoint",
                "ec2:ModifyVpcEndpoint"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*",
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:subnet/*"
            ]
        },
        {
             "Sid": "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
             "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateVpcEndpoint"
                },
```

```
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutySecurityGroupManagementPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/GuardDutyManaged": "*"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupForVpcPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        },
        {
            "Sid": "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
```

```
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSecurityGroup"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateEksAddonPolicy",
            "Effect": "Allow",
            "Action": "eks:CreateAddon",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEksAddonManagementPolicy",
            "Effect": "Allow",
            "Action": [
                "eks:DeleteAddon",
                "eks:UpdateAddon",
                "eks:DescribeAddon"
            ],
            "Resource": "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
        },
        {
            "Sid": "GuardDutyEksClusterTagResourcePolicy",
            "Effect": "Allow",
            "Action": "eks:TagResource",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEcsPutAccountSettingsDefaultPolicy",
            "Effect": "Allow",
```

```
            "Action": "ecs:PutAccountSettingDefault",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecs:account-setting": [
                        "guardDutyActivate"
                    ]
                 }
            }
        },
        {
            "Sid": "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeAssociation",
                "ssm:DeleteAssociation",
                "ssm:UpdateAssociation",
                "ssm:CreateAssociation",
                "ssm:StartAssociationsOnce"
            ],
            "Resource": "arn:aws:ssm:*:*:association/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
        },
        {
            "Sid": "SsmAddTagsToResourcePermission",
            "Effect": "Allow",
            "Action": [
                "ssm:AddTagsToResource"
            ],
            "Resource": "arn:aws:arn:aws:ssm:*:*:association/*",
            "Condition":{
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                },
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
```

```
        },
        {
            "Sid": "SsmCreateUpdateAssociationInstanceDocumentPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateAssociation",
                "ssm:UpdateAssociation"
            ],
            "Resource": "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
        },
        {
            "Sid": "SsmSendCommandPermission",
            "Effect": "Allow",
            "Action": "ssm:SendCommand",
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
            ]
        },
        {
            "Sid": "SsmGetCommandStatus",
            "Effect": "Allow",
            "Action": "ssm:GetCommandInvocation",
            "Resource": "*"
        }
    ]
}
```

Nachfolgend wird die der serviceverknüpften Rolle `AWSServiceRoleForAmazonGuardDuty` zugeordnete Vertrauensrichtlinie gezeigt:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
```

```
  ]
}
```

Einzelheiten zu Aktualisierungen der `AmazonGuardDutyServiceRolePolicy` Richtlinie finden Sie unterGuardDuty Aktualisierungen AWS verwalteter Richtlinien. Abonnieren Sie den RSS-Feed auf der Dokumentverlauf Seite, um automatische Benachrichtigungen über Änderungen an dieser Richtlinie zu erhalten.

Erstellen einer serviceverknüpften Rolle für GuardDuty

Die `AWSServiceRoleForAmazonGuardDuty` dienstverknüpfte Rolle wird automatisch erstellt, wenn Sie sie GuardDuty zum ersten Mal oder GuardDuty in einer unterstützten Region aktivieren, in der sie zuvor nicht aktiviert war. Sie können die serviceverknüpfte Rolle auch manuell mithilfe der IAM-Konsole, der oder der AWS CLI IAM-API erstellen.

> **Important**
>
> Die dienstverknüpfte Rolle, die für das GuardDuty delegierte Administratorkonto erstellt wurde, gilt nicht für die Mitgliedskonten. GuardDuty

Sie müssen Berechtigungen konfigurieren, damit ein IAM-Prinzipal (z. B. ein Benutzer, eine Gruppe oder eine Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Damit die `AWSServiceRoleForAmazonGuardDuty` dienstverknüpfte Rolle erfolgreich erstellt werden kann, muss der IAM-Prinzipal, den Sie GuardDuty mit verwenden, über die erforderlichen Berechtigungen verfügen. Um die erforderlichen Berechtigungen zu erteilen, weisen Sie diesem -Benutzer bzw. dieser-Gruppe oder -Rolle die folgende Richtlinie zu:

> **Note**
>
> Ersetzen Sie die *`Beispielkonto-ID`* im folgenden Beispiel durch Ihre tatsächliche AWS Konto-ID.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "guardduty:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

Weitere Informationen zum Erstellen von IAM-Rollen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Bearbeitung einer serviceverknüpften Rolle für GuardDuty

GuardDuty erlaubt es Ihnen nicht, die `AWSServiceRoleForAmazonGuardDuty` dienstbezogene Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für GuardDuty

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird.

> **Important**
>
> Wenn Sie den Malware Protection aktiviert haben, wird `AWSServiceRoleForAmazonGuardDuty` nicht automatisch `AWSServiceRoleForAmazonGuardDutyMalwareProtection` löschen. Wenn Sie `AWSServiceRoleForAmazonGuardDutyMalwareProtection` löschen möchten, finden Sie Informationen unter Löschen einer serviceverknüpften Rolle für Malware Protection.

Sie müssen sie zunächst GuardDuty in allen Regionen deaktivieren, in denen sie aktiviert ist, um die `AWSServiceRoleForAmazonGuardDuty` zu löschen. Wenn der GuardDuty Dienst nicht deaktiviert ist, wenn Sie versuchen, die mit dem Dienst verknüpfte Rolle zu löschen, schlägt das Löschen fehl. Weitere Informationen finden Sie unter Aussetzen oder Deaktivieren GuardDuty.

Wenn Sie ihn deaktivieren GuardDuty, wird `AWSServiceRoleForAmazonGuardDuty` er nicht automatisch gelöscht. Wenn Sie es GuardDuty erneut aktivieren, wird das Bestehende verwendet`AWSServiceRoleForAmazonGuardDuty`.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die IAM-API AWS CLI, um die `AWSServiceRoleForAmazonGuardDuty` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Wird unterstützt AWS-Regionen

Amazon GuardDuty unterstützt die Verwendung der `AWSServiceRoleForAmazonGuardDuty` serviceverknüpften Rolle überall AWS-Regionen dort, wo sie verfügbar GuardDuty ist. Eine Liste der Regionen, in denen GuardDuty das Produkt derzeit verfügbar ist, finden Sie unter GuardDuty Amazon-Endpunkte und Kontingente in der Allgemeine Amazon Web Services-Referenz.

Serviceverknüpfte Rollenberechtigungen für den Malware Protection

Der Malware Protection verwendet die serviceverknüpfte Rolle (SLR) namens `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Mit dieser Spiegelreflexkamera

kann Malware Protection agentenlose Scans durchführen, um Malware in Ihrem Konto zu erkennen. GuardDuty Es ermöglicht GuardDuty die Erstellung eines EBS-Volume-Snapshots in Ihrem Konto und die gemeinsame Nutzung dieses Snapshots mit dem GuardDuty Dienstkonto. Nach der GuardDuty Auswertung des Snapshots werden die abgerufenen EC2-Instance- und Container-Workload-Metadaten in die Ergebnisse des Malware-Schutzes aufgenommen. Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` vertraut dem Service `malware-protection.guardduty.amazonaws.com`, sodass dieser die Rolle annehmen kann.

Die Berechtigungsrichtlinien für diese Rolle helfen Malware Protection dabei, die folgenden Aufgaben auszuführen:

- Verwenden Sie Amazon Elastic Compute Cloud (Amazon EC2) -Aktionen, um Informationen über Ihre Amazon EC2 EC2-Instances, Volumes und Snapshots abzurufen. Malware Protection gewährt auch die Erlaubnis, auf die Amazon EKS- und Amazon ECS-Cluster-Metadaten zuzugreifen.
- Erstellen Sie Snapshots für EBS-Volumes, bei denen das `GuardDutyExcluded`-Tag nicht auf `true` gesetzt ist. Standardmäßig werden die Snapshots mit einem `GuardDutyScanId`-Tag erstellt. Entfernen Sie dieses Tag nicht, da Malware Protection sonst keinen Zugriff auf die Snapshots hat.

  > **Important**
  >
  > Wenn Sie das `GuardDutyExcluded` auf setzen`true`, kann der GuardDuty Dienst in future nicht mehr auf diese Snapshots zugreifen. Dies liegt daran, dass die anderen Anweisungen in dieser dienstbezogenen Rolle GuardDuty verhindern, dass Aktionen für die Snapshots ausgeführt werden, für die der Wert auf gesetzt ist. `GuardDutyExcluded` `true`

- Lassen Sie das Teilen und Löschen von Snapshots nur zu, wenn das `GuardDutyScanId`-Tag existiert und das `GuardDutyExcluded`-Tag nicht auf `true` gesetzt ist.

  > **Note**
  >
  > Erlaubt Malware Protection nicht, die Snapshots zu veröffentlichen.

- Greifen Sie auf vom Kunden verwaltete Schlüssel zu, mit Ausnahme von Schlüsseln, für die ein `GuardDutyExcluded` Tag auf gesetzt ist`true`, und rufen Sie auf, `CreateGrant` um anhand des verschlüsselten Snapshots, der mit dem Dienstkonto geteilt wird, ein verschlüsseltes EBS-Volume

zu erstellen und darauf zuzugreifen. GuardDuty Eine Liste der GuardDuty Dienstkonten für jede Region finden Sie unterGuardDuty Dienstkonten von AWS-Region.

- Greifen Sie auf die CloudWatch Kundenprotokolle zu, um die Protokollgruppe „Malware-Schutz“ zu erstellen und die Ereignisprotokolle der Malware-Suche der `/aws/guardduty/malware-scan-events` Protokollgruppe zuzuordnen.
- Lassen Sie den Kunden entscheiden, ob er die Snapshots, auf denen Malware erkannt wurde, in seinem Konto behalten möchte. Wenn beim Scan Malware erkannt wird, ermöglicht die mit dem Dienst verknüpfte Rolle GuardDuty das Hinzufügen von zwei Tags zu Snapshots: und. `GuardDutyFindingDetected` `GuardDutyExcluded`

  > **Note**
  >
  > Das `GuardDutyFindingDetected`-Tag gibt an, dass die Snapshots Malware enthalten.

- Ermitteln Sie, ob ein Volume mit einem von EBS verwalteten Schlüssel verschlüsselt ist. GuardDuty führt die `DescribeKey` Aktion durch, um den `key Id` von EBS verwalteten Schlüssel in Ihrem Konto zu ermitteln.
- Rufen Sie den Snapshot der EBS-Volumes, verschlüsselt mit Von AWS verwalteter Schlüssel, von Ihrem ab AWS-Konto und kopieren Sie ihn in den. GuardDuty Dienstkonto Zu diesem Zweck verwenden wir die Berechtigungen `GetSnapshotBlock` und. `ListSnapshotBlocks` GuardDuty scannt dann den Snapshot im Dienstkonto. Derzeit ist die Unterstützung des Malware-Schutzes für das Scannen von EBS-Volumes, die mit verschlüsselt sind, Von AWS verwalteter Schlüssel möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter Verfügbarkeit regionsspezifischer Feature.
- Erlauben Sie Amazon EC2, AWS KMS im Namen von Malware Protection mehrere kryptografische Aktionen mit vom Kunden verwalteten Schlüsseln durchzuführen. Aktionen wie `kms:ReEncryptTo` und `kms:ReEncryptFrom` sind erforderlich, um die Snapshots zu teilen, die mit den vom Kunden verwalteten Schlüsseln verschlüsselt sind. Es sind nur die Schlüssel zugänglich, für die das `GuardDutyExcluded`-Tag nicht auf `true` festgelegt ist.

Die Rolle ist mit der folgenden AWS -verwalteten Richtlinie namens `AmazonGuardDutyMalwareProtectionServiceRolePolicy` konfiguriert.

```
{
    "Version": "2012-10-17",
    "Statement": [{
```

```
            "Sid": "DescribeAndListPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ecs:ListClusters",
                "ecs:ListContainerInstances",
                "ecs:ListTasks",
                "ecs:DescribeTasks",
                "eks:DescribeCluster"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateSnapshotVolumeConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:volume/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "CreateSnapshotConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyScanId"
                }
            }
        },
        {
            "Sid": "CreateTagsPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:*/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSnapshot"
```

```
                }
            }
        },
        {
            "Sid": "AddTagsToSnapshotPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyExcluded",
                        "GuardDutyFindingDetected"
                    ]
                }
            }
        },
        {
            "Sid": "DeleteAndShareSnapshotPermission",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot",
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "PreventPublicAccessToSnapshotPermission",
            "Effect": "Deny",
            "Action": [
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
```

```
            "Condition": {
                "StringEquals": {
                    "ec2:Add/group": "all"
                }
            }
        },
        {
            "Sid": "CreateGrantPermission",
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:ebs:id": "snap-*"
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Decrypt",
                        "CreateGrant",
                        "GenerateDataKeyWithoutPlaintext",
                        "ReEncryptFrom",
                        "ReEncryptTo",
                        "RetireGrant",
                        "DescribeKey"
                    ]
                },
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Sid": "ShareSnapshotKMSPermission",
            "Effect": "Allow",
            "Action": [
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "StringLike": {
```

```
                    "kms:ViaService": "ec2.*.amazonaws.com"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "DescribeKeyPermission",
            "Effect": "Allow",
            "Action": "kms:DescribeKey",
            "Resource": "arn:aws:kms:*:*:key/*"
        },
        {
            "Sid": "GuardDutyLogGroupPermission",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:CreateLogGroup",
                "logs:PutRetentionPolicy"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
        },
        {
            "Sid": "GuardDutyLogStreamPermission",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
        },
        {
            "Sid": "EBSDirectAPIPermissions",
            "Effect": "Allow",
            "Action": [
                "ebs:GetSnapshotBlock",
                "ebs:ListSnapshotBlocks"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/GuardDutyScanId": "*"
```

```
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        }
    ]
}
```

Nachfolgend wird die der serviceverknüpften Rolle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` zugeordnete Vertrauensrichtlinie gezeigt:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Erstellen einer servicegebundenen Rolle für Malware Protection

Die serviceverknüpfte Rolle namens `AWSServiceRoleForAmazonGuardDutyMalwareProtection` wird automatisch erstellt, wenn Sie Malware Protection zum ersten Mal aktivieren oder Malware Protection in einer unterstützten Region aktivieren, in der der Service zuvor nicht aktiviert war. Sie können die serviceverknüpfte Rolle namens `AWSServiceRoleForAmazonGuardDutyMalwareProtection` auch manuell erstellen, indem Sie die IAM-Konsole, die CLI oder die IAM-API verwenden.

> **Note**
>
> Wenn Sie neu bei Amazon sind GuardDuty, ist der Malware-Schutz standardmäßig automatisch aktiviert.

> **Important**
>
> Die dienstbezogene Rolle, die für das delegierte GuardDuty Administratorkonto erstellt wurde, gilt nicht für die GuardDuty Mitgliedskonten.

Sie müssen Berechtigungen konfigurieren, damit ein IAM-Prinzipal (z. B. ein Benutzer, eine Gruppe oder eine Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Damit die `AWSServiceRoleForAmazonGuardDutyMalwareProtection` dienstverknüpfte Rolle erfolgreich erstellt werden kann, muss die IAM-Identität, die Sie GuardDuty mit verwenden, über die erforderlichen Berechtigungen verfügen. Um die erforderlichen Berechtigungen zu erteilen, weisen Sie diesem -Benutzer bzw. dieser-Gruppe oder -Rolle die folgende Richtlinie zu:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

Weitere Informationen zum Erstellen von IAM-Rollen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Malware Protection

Malware Protection lässt die Bearbeitung der serviceverknüpften Rolle namens `AWSServiceRoleForAmazonGuardDutyMalwareProtection` nicht zu. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Malware Protection

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird.

> **Important**
>
> Sie müssen Malware Protection zunächst in allen aktivierten Regionen deaktivieren, um `AWSServiceRoleForAmazonGuardDutyMalwareProtection` löschen zu können. Wenn Sie versuchen, die serviceverknüpfte Rolle zu löschen und Malware Protection noch nicht deaktiviert wurde, schlägt das Löschen fehl. Weitere Informationen finden Sie unter Um den GuardDuty -initiierten Malware-Scan zu aktivieren oder zu deaktivieren.

Wenn Sie Deaktivieren wählen, um Malware Protection zu beenden, wird die `AWSServiceRoleForAmazonGuardDutyMalwareProtection` nicht automatisch

gelöscht. Wenn Sie dann „Aktivieren“ wählen, um den Malware Protection-Dienst erneut zu starten, GuardDuty wird der vorhandene Dienst wieder verwendet. `AWSServiceRoleForAmazonGuardDutyMalwareProtection`

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die AWS CLI oder die IAM-API, um die `AWSServiceRoleForAmazonGuardDutyMalwareProtection` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Wird unterstützt AWS-Regionen

Amazon GuardDuty unterstützt die Verwendung der `AWSServiceRoleForAmazonGuardDutyMalwareProtection` serviceverknüpften Rolle in allen Bereichen, in AWS-Regionen denen Malware-Schutz verfügbar ist.

Eine Liste der Regionen, in denen GuardDuty das Produkt derzeit verfügbar ist, finden Sie unter GuardDuty Amazon-Endpunkte und Kontingente in der Allgemeine Amazon Web Services-Referenz.

> **Note**
>
> Der Malware-Schutz ist derzeit in AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) nicht verfügbar.

AWS verwaltete Richtlinien für Amazon GuardDuty

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAM-Benutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Dienste fügen einer AWS verwalteten Richtlinie gelegentlich zusätzliche Berechtigungen hinzu, um neue Funktionen zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die

Richtlinie angehängt ist. Es ist sehr wahrscheinlich, dass Dienste eine AWS verwaltete Richtlinie aktualisieren, wenn eine neue Funktion eingeführt wird oder wenn neue Operationen verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess

Sie können die `AmazonGuardDutyFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen, die einem Benutzer vollen Zugriff auf alle GuardDuty Aktionen gewähren.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `GuardDuty`— Ermöglicht Benutzern vollen Zugriff auf alle GuardDuty Aktionen.
- `IAM`— Ermöglicht Benutzern, die GuardDuty dienstbezogene Rolle zu erstellen. Auf diese Weise kann ein GuardDuty Administrator GuardDuty Mitgliedskonten aktivieren.
- `Organizations`— Ermöglicht Benutzern, einen delegierten Administrator zu benennen und Mitglieder für eine GuardDuty Organisation zu verwalten.

Die Berechtigung zum Ausführen einer `iam:GetRole`-Aktion für `AWSServiceRoleForAmazonGuardDutyMalwareProtection` legt fest, ob die serviceverknüpfte Rolle (SLR) für Malware Protection in einem Konto vorhanden ist.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonGuardDutyFullAccessSid1",
```

```
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleSid1",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "guardduty.amazonaws.com",
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "ActionsForOrganizationsSid1",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IamGetRoleSid1",
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

AWS verwaltete Richtlinie: AmazonGuardDutyReadOnlyAccess

Sie können die `AmazonGuardDutyReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Benutzern nur Leseberechtigungen, die es Benutzern ermöglichen, GuardDuty Ergebnisse und Details Ihrer GuardDuty Organisation einzusehen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `GuardDuty`— Ermöglicht Benutzern, GuardDuty Ergebnisse einzusehen und API-Operationen durchzuführen, die mit `GetList`, oder beginnen. `Describe`
- `Organizations`— Ermöglicht Benutzern das Abrufen von Informationen über Ihre GuardDuty Organisationskonfiguration, einschließlich Details zum delegierten Administratorkonto.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:Describe*",
                "guardduty:Get*",
                "guardduty:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

AWS verwaltete Richtlinie: AmazonGuardDutyServiceRolePolicy

Sie können `AmazonGuardDutyServiceRolePolicy` nicht an Ihre IAM-Entitäten anhängen. Diese AWS verwaltete Richtlinie ist einer dienstbezogenen Rolle zugeordnet, mit der GuardDuty Sie Aktionen in Ihrem Namen ausführen können. Weitere Informationen finden Sie unter Mit dem Dienst verknüpfte Rollenberechtigungen für GuardDuty.

GuardDuty Aktualisierungen AWS verwalteter Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die GuardDuty seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS-Feed auf der Seite GuardDuty Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Verwenden Sie AWS Systems Manager Aktionen, um SSM-Verknüpfungen auf Amazon EC2-Instances zu verwalten, wenn Sie GuardDuty Runtime Monitoring mit automatisiertem Agenten für Amazon EC2 aktivieren. Wenn die GuardDuty automatische Agentenkonfiguration deaktiviert ist, werden nur die EC2-Instances GuardDuty berücksichtigt, die über ein Inclusion-Tag (:) verfügen. `GuardDutyManaged true`	26. März 2024
AmazonGuardDutyServiceRolePolicy – Aktualisi	GuardDuty hat eine neue Berechtigung hinzugefü	9. Februar 2024

Änderung	Beschreibung	Datum
erung auf eine bestehende Richtlinie.	gtorganization:DescribeOrganization , um die Organisations-ID des gemeinsamen Amazon VPC-Kontos abzurufen und die Amazon VPC-Endpunktrichtlinie mit der Organisations-ID festzulegen.	
AmazonGuardDutyMalwareProtectionServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Der Malware-Schutz hat zwei zusätzliche Berechtigungen hinzugefügtGetSnapshotBlock : Sie ListSnapshotBlocks können den Snapshot eines EBS-Volumes (verschlüsselt mit Von AWS verwalteter Schlüssel) von Ihrem Computer abrufen AWS-Konto und in das GuardDuty Dienstkonto kopieren, bevor der Malware-Scan gestartet wird.	25. Januar 2024
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Neue Berechtigungen wurden hinzugefügt, um das Hinzufügen von guardduty Activate Amazon ECS-Kontoeinstellungen und das Ausführen von Listen- und Beschreibungsvorgängen auf Amazon ECS-Clustern zu ermöglichen GuardDuty .	26. November 2023

Änderung	Beschreibung	Datum
AmazonGuardDutyReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	GuardDuty hat eine neue Richtlinie für `organizations` to hinzugefügt `ListAccounts` .	16. November 2023
AmazonGuardDutyFullAccess – Aktualisierung auf eine bestehende Richtlinie	GuardDuty hat eine neue Richtlinie für `organizations` to hinzugefügt `ListAccounts` .	16. November 2023
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	GuardDuty neue Berechtigungen hinzugefügt, um die kommende GuardDuty EKS Runtime Monitoring-Funktion zu unterstützen.	08. März 2023

Änderung	Beschreibung	Datum
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	GuardDuty hat neue Berechtigungen hinzugefügt, um die Erstellung GuardDuty einer dienstbezogenen Rolle für den Malware-Schutz zu ermöglichen. Dies wird dazu beitragen, den Prozess der Aktivierung des Malware-Schutzes zu GuardDuty rationalisieren. GuardDuty kann jetzt die folgende IAM-Aktion ausführen: `{ "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com" } } }`	21. Februar 2023
AmazonGuardDutyFullAccess – Aktualisierung auf eine bestehende Richtlinie	GuardDuty ARN für `iam:GetRole` to aktualisiert`*AWSServiceRoleForAmazonGuardDutyMalwareProtection` .	26. Juli 2022

Änderung	Beschreibung	Datum
AmazonGuardDutyFullAccess – Aktualisierung auf eine bestehende Richtlinie	GuardDuty Es wurde eine neue hinzugefügt`AWSServiceName` , um die Erstellung einer dienstbezogenen Rolle mithilfe des `iam:CreateServiceLinkedRole` GuardDuty Malware-Schutzdienstes zu ermöglichen. GuardDuty kann jetzt die `iam:GetRole` Aktion ausführen, für `AWSServiceRole` die Informationen abgerufen werden sollen.	26. Juli 2022

Änderung	Beschreibung	Datum
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	GuardDuty neue Berechtigungen hinzugefügt, um die Verwendung von Amazon EC2 EC2-Netzwerkaktionen zur Verbesserung der Ergebnisse zu ermöglichen GuardDuty . GuardDuty kann jetzt die folgenden EC2-Aktionen ausführen, um Informationen darüber zu erhalten, wie Ihre EC2-Instances kommunizieren. Diese Informationen werden verwendet, um die Genauigkeit der Erkenntnisse zu verbessern. • `ec2:DescribeVpcEndpoints` • `ec2:DescribeSubnets` • `ec2:DescribeVpcPeeringConnections` • `ec2:DescribeTransitGatewayAttachments`	3. August 2021
GuardDuty hat begonnen, Änderungen zu verfolgen	GuardDuty hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	3. August 2021

Fehlerbehebung Amazon GuardDuty Amazon-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit GuardDuty IAM auftreten können.

Themen

Ich bin nicht berechtigt, eine Aktion durchzuführen in GuardDuty

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `guardduty:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 guardduty:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `guardduty:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam: PassRole auszuführen.

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an GuardDuty diese Person übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in auszuführen. GuardDuty Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine GuardDuty Ressourcen ermöglichen.

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen GuardDuty unterstützt werden, finden Sie unterSo GuardDuty arbeitet Amazon mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Konformitätsvalidierung für Amazon GuardDuty

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

  > **Note**
  >
  > AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.

- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Ausfallsicherheit bei Amazon GuardDuty

Im Zentrum der globalen AWS-Infrastruktur stehen die AWS-Regionen und -Availability Zones. Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen über AWS-Regionen und -Availability Zones finden Sie unter Globale AWS-Infrastruktur.

Sicherheit der Infrastruktur in Amazon GuardDuty

Als verwalteter Service ist Amazon GuardDuty durch die globale Netzwerksicherheit von AWS geschützt. Informationen zu AWS-Sicherheitsservices und wie AWS die Infrastruktur schützt, finden Sie unter AWS-Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf GuardDuty zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

AWS-Serviceintegrationen mit GuardDuty

GuardDuty kann mit anderen AWS-Sicherheits-Services integriert werden. Diese Services können Daten von GuardDuty aufnehmen, sodass Sie die Erkenntnisse auf neue Weise betrachten können. Lesen Sie die folgenden Integrationsoptionen, um mehr darüber zu erfahren, wie jeder Service mit GuardDuty funktioniert.

Integration von GuardDuty mit AWS Security Hub

AWS Security Hub sammelt Sicherheitsdaten aus allen Ihren AWS-Konten, Services und unterstützten Partnerprodukten von Drittanbietern, um den Sicherheitsstatus Ihrer Umgebung gemäß Industriestandards und bewährten Methoden zu bewerten. Security Hub bewertet nicht nur Ihren Sicherheitsstatus, sondern bietet auch einen zentralen Ort für Erkenntnisse aus all Ihren integrierten AWS-Services und AWS-Partnerprodukten. Durch die Aktivierung von Security Hub mit GuardDuty können GuardDuty-Erkenntnisdaten automatisch von Security Hub aufgenommen werden.

Weitere Informationen zur Verwendung von Security Hub mit GuardDuty finden Sie unter Integration mit AWS Security Hub.

Integration von GuardDuty mit Amazon Detective

Amazon Detective verwendet Protokolldaten aus all Ihren AWS-Konten, um Datenvisualisierungen für Ihre Ressourcen und IP-Adressen zu erstellen, die mit Ihrer Umgebung interagieren. Die Visualisierungen von Detective helfen Ihnen dabei, Sicherheitsprobleme schnell und einfach zu untersuchen. Sobald beide Services aktiviert sind, können Sie von GuardDuty-Erkenntnisdetails zu Informationen in der Detective-Konsole wechseln.

Weitere Informationen zur Verwendung von Security Hub mit GuardDuty finden Sie unter Integration mit Amazon Detective.

Integration mit AWS Security Hub

AWS Security Hub liefert einen umfassenden Überblick über den Sicherheitsstatus in AWS und hilft Ihnen dabei, Ihre Umgebung anhand von Sicherheitsstandards und bewährten Methoden der Branche zu überprüfen. Security Hub sammelt Sicherheitsdaten von AWS Konten, Diensten und unterstützten Partnerprodukten von Drittanbietern und hilft Ihnen dabei, Ihre Sicherheitstrends zu analysieren und die Sicherheitsprobleme mit der höchsten Priorität zu identifizieren.

Die GuardDuty Amazon-Integration mit Security Hub ermöglicht es Ihnen, Ergebnisse von an Security Hub GuardDuty zu senden. Der Security Hub kann diese Erkenntnisse dann in die Analyse Ihres Sicherheitsniveaus einbeziehen.

Inhalt

So GuardDuty sendet Amazon Ergebnisse an AWS Security Hub

AWS Security Hub In werden Sicherheitsprobleme als Ergebnisse erfasst. Einige Ergebnisse stammen aus Problemen, die von anderen AWS Diensten oder von Drittanbietern entdeckt wurden. Security Hub verwendet ebenfalls verschiedene Regeln, um Sicherheitsprobleme zu erkennen und Ergebnisse zu generieren.

Security Hub bietet Tools zur Verwaltung von Erkenntnissen aus all diesen Quellen. Sie können Listen mit Erkenntnissen anzeigen und filtern und Details zu einer Erkenntnis anzeigen. Weitere Informationen finden Sie unter Anzeigen der Erkenntnisse im AWS Security Hub -Benutzerhandbuch. Sie können auch den Status einer Untersuchung zu einer Erkenntnis nachverfolgen. Weitere Informationen finden Sie unter Ergreifen von Maßnahmen zu Erkenntnissen im AWS Security Hub -Benutzerhandbuch.

Alle Ergebnisse in Security Hub verwenden ein standardmäßiges JSON-Format, das AWS Security Finding Format (ASFF). Das ASFF enthält Details über die Ursache des Problems, die betroffenen Ressourcen und den aktuellen Status der Erkenntnis. Siehe AWS -Security Finding-Format (ASFF) im AWS Security Hub -Leitfaden.

Amazon GuardDuty ist einer der AWS Dienste, der Ergebnisse an Security Hub sendet.

Arten von Ergebnissen, die GuardDuty an Security Hub gesendet werden

Sobald Sie Security Hub in demselben Konto innerhalb desselben aktiviert GuardDuty haben AWS-Region, GuardDuty werden alle generierten Ergebnisse an Security Hub gesendet. Diese Ergebnisse werden mit dem Security Finding Format (ASFF) an AWS Security Hub gesendet. In ASFF gibt das `Types`-Feld die Art der Erkenntnis an.

Latenz beim Senden neuer Ergebnisse

Wenn ein neues Ergebnis GuardDuty erstellt wird, wird es normalerweise innerhalb von fünf Minuten an Security Hub gesendet.

Wiederholen, wenn der Security Hub nicht verfügbar ist

Wenn Security Hub nicht verfügbar ist, wird GuardDuty erneut versucht, die Ergebnisse zu senden, bis sie empfangen werden.

Aktualisieren von vorhandenen Erkenntnissen in Security Hub

Nachdem es ein Ergebnis an Security Hub gesendet hat, GuardDuty sendet es Updates, um zusätzliche Beobachtungen der Findungsaktivität widerzuspiegeln, an Security Hub. Die neuen Beobachtungen dieser Ergebnisse werden basierend auf den Schritt 5 — Aktualisierungshäufigkeit exportieren Einstellungen in Ihrem an Security Hub gesendet AWS-Konto.

Wenn Sie einen Befund archivieren oder die Archivierung aufheben, GuardDuty wird dieser Befund nicht an Security Hub gesendet. Manuell dearchivierte Ergebnisse, die später aktiv werden, werden nicht an Security Hub gesendet. GuardDuty

GuardDuty Ergebnisse anzeigen in AWS Security Hub

Um Ihre GuardDuty Ergebnisse in Security Hub einzusehen, wählen Sie auf der Übersichtsseite die Option Ergebnisse unter Amazon anzeigen GuardDuty aus. Alternativ können Sie im Navigationsbereich die Option Ergebnisse auswählen und die Ergebnisse so filtern, dass nur GuardDuty Ergebnisse angezeigt werden, indem Sie das Feld Produktname: mit dem Wert von auswählen`GuardDuty`.

Interpretieren von GuardDuty Fundnamen in AWS Security Hub

GuardDuty sendet die Ergebnisse mithilfe des AWS Security Finding Formats (ASFF) an Security Hub. In ASFF gibt das `Types`-Feld die Art der Erkenntnis an. ASFF-Typen verwenden ein anderes

Benennungsschema als GuardDuty Typen. In der folgenden Tabelle sind alle GuardDuty Findetypen mit ihren ASFF-Gegenstücken aufgeführt, so wie sie in Security Hub erscheinen.

> **Note**
>
> Für einige GuardDuty Ergebnisarten weist Security Hub unterschiedliche ASFF-Suchnamen zu, je nachdem, ob die Ressourcenrolle des Ergebnisdetails ACTOR oder TARGET war. Weitere Informationen finden Sie unter Erkenntnisdetails.

GuardDuty Findetyp	ASFF-Ergebnistyp
Backdoor:EC2/C&CActivity.B	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B
Backdoor:EC2/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS
Backdoor:EC2/DenialOfService.Dns	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Dns
Backdoor:EC2/DenialOfService.Tcp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Tcp
Backdoor:EC2/DenialOfService.Udp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts
Backdoor:EC2/DenialOfService.UnusualProtocol	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol
Backdoor:EC2/Spambot	TTPs/Command and Control/Backdoor:EC2-Spambot
Behavior:EC2/NetworkPortUnusual	Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual

GuardDuty Findetyp	ASFF-Ergebnistyp
Behavior:EC2/TrafficVolumeUnusual	Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual
Backdoor:Lambda/C&CActivity.B	TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B
Backdoor:Runtime/C&CActivity.B	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B
Backdoor:Runtime/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS
CredentialAccess:IAMUser/AnomalousBehavior	TTPs/Credential Access/IAMUser-AnomalousBehavior
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulBruteForce
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulLogin
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.FailedLogin
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.SuccessfulLogin
CredentialAccess:RDS/TorIPCaller.FailedLogin	TTPs/Credential Access/RDS-TorIPCaller.FailedLogin
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-TorIPCaller.SuccessfulLogin

GuardDuty Findetyp	ASFF-Ergebnistyp
CryptoCurrency:EC2/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B
CryptoCurrency:EC2/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B!DNS
DefenseEvasion:EC2/UnusualDNSResolver	TTPs/DefenseEvasion/EC2:Unusual-DNS-Resolver
DefenseEvasion:EC2/UnusualDoHActivity	TTPs/DefenseEvasion/EC2:Unusual-DoH-Activity
DefenseEvasion:EC2/UnusualDoTActivity	TTPs/DefenseEvasion/EC2:Unusual-DoT-Activity
DefenseEvasionSuchtyp ----SEP----:IAMUser/AnomalousBehavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/PtraceAntiDebugging	TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging
DefenseEvasion:Runtime/SuspiciousCommand	TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand

GuardDuty Findetyp	ASFF-Ergebnistyp
Entdeckung: IamUser/ AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
Discovery:S3/AnomalousBehavior	TTPs/Discovery:S3-AnomalousBehavior
Discovery:S3/BucketEnumeration.Unusual	TTPs/Discovery:S3-BucketEnumeration.Unusual
Discovery:S3/MaliciousIPCaller.Custom	TTPs/Discovery:S3-MaliciousIPCaller.Custom
Discovery:S3/TorIPCaller	TTPs/Discovery:S3-TorIPCaller
Discovery:S3/MaliciousIPCaller	TTPs/Discovery:S3-MaliciousIPCaller
Execution:Kubernetes/AnomalousBehavior.ExecInPod	TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer
Execution:EC2/MaliciousFile	TTPs/Execution/Execution:EC2-MaliciousFile
Execution:ECS/MaliciousFile	TTPs/Execution/Execution:ECS-MaliciousFile

GuardDuty Findetyp	ASFF-Ergebnistyp
Execution:Kubernetes/MaliciousFile	TTPs/Execution/Execution:Kubernetes-MaliciousFile
Execution:Container/MaliciousFile	TTPs/Execution/Execution:Container-MaliciousFile
Execution:EC2/SuspiciousFile	TTPs/Execution/Execution:EC2-SuspiciousFile
Execution:ECS/SuspiciousFile	TTPs/Execution/Execution:ECS-SuspiciousFile
Execution:Kubernetes/SuspiciousFile	TTPs/Execution/Execution:Kubernetes-SuspiciousFile
Execution:Container/SuspiciousFile	TTPs/Execution/Execution:Container-SuspiciousFile
Execution:Runtime/MaliciousFileExecuted	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted
Execution:Runtime/NewBinaryExecuted	TTPs/Execution/Execution:Runtime-NewBinaryExecuted
Execution:Runtime/NewLibraryLoaded	TTPs/Execution/Execution:Runtime-NewLibraryLoaded
Execution:Runtime/ReverseShell	TTPs/Execution/Execution:Runtime-ReverseShell
Execution:Runtime/SuspiciousCommand	TTPs/Execution/Execution:Runtime-SuspiciousCommand
Execution:Runtime/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual

GuardDuty Findetyp	ASFF-Ergebnistyp
Exfiltration:S3/MaliciousIPCaller	TTPs/Exfiltration:S3-MaliciousIPCaller
Impact:EC2/AbusedDomainRequest.Reputation	TTPs/Impact:EC2-AbusedDomainRequest.Reputation
Impact:EC2/BitcoinDomainRequest.Reputation	TTPs/Impact:EC2-BitcoinDomainRequest.Reputation
Impact:EC2/MaliciousDomainRequest.Reputation	TTPs/Impact:EC2-MaliciousDomainRequest.Reputation
Impact:EC2/PortSweep	TTPs/Impact/Impact:EC2-PortSweep
Impact:EC2/SuspiciousDomainRequest.Reputation	TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation
Impact:EC2/WinRMBruteForce	TTPs/Impact/Impact:EC2-WinRMBruteForce
Auswirkung: iamUser/ AnomalousBehavior	TTPs/Impact/IAMUser-AnomalousBehavior
Impact:Runtime/AbusedDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation
Impact:Runtime/BitcoinDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-BitcoinDomainRequest.Reputation
Impact:Runtime/CryptoMinerExecuted	TTPs/Impact/Impact:Runtime-CryptoMinerExecuted
Impact:Runtime/MaliciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation
Impact:Runtime/SuspiciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-SuspiciousDomainRequest.Reputatio
Impact:S3/AnomalousBehavior.Delete	TTPs/Impact:S3-AnomalousBehavior.Delete

GuardDuty Findetyp	ASFF-Ergebnistyp
Impact:S3/AnomalousBehavior.Permission	TTPs/Impact:S3-AnomalousBehavior.Permission
Impact:S3/AnomalousBehavior.Write	TTPs/Impact:S3-AnomalousBehavior.Write
Impact:S3/ObjectDelete.Unusual	TTPs/Impact:S3-ObjectDelete.Unusual
Impact:S3/PermissionsModification.Unusual	TTPs/Impact:S3-PermissionsModification.Unusual
Impact:S3/MaliciousIPCaller	TTPs/Impact:S3-MaliciousIPCaller
InitialAccessAuswirkung: IAMUser/ ----SEP----:IAMUser/ AnomalousBehavior	TTPs/Initial Access/IAMUser-AnomalousBehavior
PenTest:IAMUser/KaliLinux	TTPs/PenTest:IAMUser/KaliLinux
PenTest:IAMUser/ParrotLinux	TTPs/PenTest:IAMUser/ParrotLinux
PenTest:IAMUser/PentooLinux	TTPs/PenTest:IAMUser/PentooLinux
PenTest:S3/KaliLinux	TTPs/PenTest:S3-KaliLinux
PenTest:S3/ParrotLinux	TTPs/PenTest:S3-ParrotLinux
PenTest:S3/PentooLinux	TTPs/PenTest:S3-PentooLinux
Persistenz: IamUser/ AnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior
Persistence:IAMUser/NetworkPermissions	TTPs/Persistence/Persistence:IAMUser-NetworkPermissions
Persistence:IAMUser/ResourcePermissions	TTPs/Persistence/Persistence:IAMUser-ResourcePermissions
Persistence:IAMUser/UserPermissions	TTPs/Persistence/Persistence:IAMUser-UserPermissions

GuardDuty Findetyp	ASFF-Ergebnistyp
Policy:IAMUser/RootCredentialUsage	TTPs/Policy:IAMUser-RootCredentialUsage
Policy:S3/AccountBlockPublicAccessDisabled	TTPs/Policy:S3-AccountBlockPublicAccessDisabled
Policy:S3/BucketAnonymousAccessGranted	TTPs/Policy:S3-BucketAnonymousAccessGranted
Policy:S3/BucketBlockPublicAccessDisabled	Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled
Policy:S3/BucketPublicAccessGranted	TTPs/Policy:S3-BucketPublicAccessGranted
PrivilegeEscalationPersistenz: IAMUser/ ----SEP----:IAMUser/ AnomalousBehavior	TTPs/Privilege Escalation/IAMUser-AnomalousBehavior
PrivilegeEscalation:IAMUser/AdministrativePermissions	TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	TTPs/AnomalousBehavior/PriviledgeEscalation:Kubernetes-RoleBindingCreated
PriviledgeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	TTPs/AnomalousBehavior/PriviledgeEscalation:Kubernetes-RoleCreated
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified
PrivilegeEscalation:Runtime/DockerSocketAccessed	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed
PrivilegeEscalation:Runtime/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape

GuardDuty Findetyp	ASFF-Ergebnistyp
PrivilegeEscalation:Runtime/UserfaultfdUsage	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-UserfaultfdUsage
Recon:EC2/PortProbeEMRUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeEMRUnprotectedPort
Recon:EC2/PortProbeUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeUnprotectedPort
Recon:EC2/Portscan	TTPs/Discovery/Recon:EC2-Portscan
Recon:IAMUser/MaliciousIPCaller	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller
Recon:IAMUser/MaliciousIPCaller.Custom	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller.Custom
Recon:IAMUser/NetworkPermissions	TTPs/Discovery/Recon:IAMUser-NetworkPermissions
Recon:IAMUser/ResourcePermissions	TTPs/Discovery/Recon:IAMUser-ResourcePermissions
Recon:IAMUser/TorIPCaller	TTPs/Discovery/Recon:IAMUser-TorIPCaller
Recon:IAMUser/UserPermissions	TTPs/Discovery/Recon:IAMUser-UserPermissions
ResourceConsumption:IAMUser/ComputeResources	Unusual Behaviors/User/ResourceConsumption:IAMUser-ComputeResources
Stealth:IAMUser/CloudTrailLoggingDisabled	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled
Stealth:IAMUser/LoggingConfigurationModified	TTPs/Defense Evasion/Stealth:IAMUser-LoggingConfigurationModified

GuardDuty Findetyp	ASFF-Ergebnistyp
Stealth:IAMUser/PasswordPolicyChange	TTPs/Defense Evasion/Stealth:IAMUser-PasswordPolicyChange
Stealth:S3/ServerAccessLoggingDisabled	TTPs/Defense Evasion/Stealth:S3-ServerAccessLoggingDisabled
Trojan:EC2/BlackholeTraffic	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic
Trojan:EC2/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic!DNS
Trojan:EC2/DGADomainRequest.B	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.B
Trojan:EC2/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.C!DNS
Trojan:EC2/DNSDataExfiltration	TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration
Trojan:EC2/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:EC2-DriveBySourceTraffic!DNS
Trojan:EC2/DropPoint	Effects/Data Exfiltration/Trojan:EC2-DropPoint
Trojan:EC2/DropPoint!DNS	Effects/Data Exfiltration/Trojan:EC2-DropPoint!DNS
Trojan:EC2/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:EC2-PhishingDomainRequest!DNS
Trojan:Lambda/BlackholeTraffic	TTPs/Command and Control/Trojan:Lambda-BlackholeTraffic
Trojan:Lambda/DropPoint	Effects/Data Exfiltration/Trojan:Lambda-DropPoint

GuardDuty Findetyp	ASFF-Ergebnistyp
Trojan:Runtime/BlackholeTraffic	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic
Trojan:Runtime/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic!DNS
Trojan:Runtime/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:Runtime-DGADomainRequest.C!DNS
Trojan:Runtime/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:Runtime-DriveBySourceTraffic!DNS
Trojan:Runtime/DropPoint	Effects/Data Exfiltration/Trojan:Runtime-DropPoint
Trojan:Runtime/DropPoint!DNS	Effects/Data Exfiltration/Trojan:Runtime-DropPoint!DNS
Trojan:Runtime/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:Runtime-PhishingDomainRequest!DNS
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:EC2-MaliciousIPCaller.Custom
UnauthorizedAccess:EC2/MetadataDNSRebind	TTPs/UnauthorizedAccess:EC2-MetadataDNSRebind
UnauthorizedAccess:EC2/RDPBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-RDPBruteForce
UnauthorizedAccess:EC2/SSHBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce
UnauthorizedAccess:EC2/TorClient	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorClient
UnauthorizedAccess:EC2/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay

GuardDuty Findetyp	ASFF-Ergebnistyp
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/UnauthorizedAccess:IAMUser-ConsoleLogin
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS
UnauthorizedAccess:IAMUser/MaliciousIPCaller	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom
UnauthorizedAccess:IAMUser/TorIPCaller	TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom
UnauthorizedAccess:Lambda/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient
UnauthorizedAccess:Lambda/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay
UnauthorizedAccess:Runtime/MetadataDNSRebind	TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind
UnauthorizedAccess:Runtime/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay

GuardDuty Findetyp	ASFF-Ergebnistyp
UnauthorizedAccess:Runtime/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom
UnauthorizedAccess:S3/TorIPCaller	TTPs/UnauthorizedAccess:S3-TorIPCaller

Typische Erkenntnis von GuardDuty

GuardDuty sendet Ergebnisse mithilfe des AWS Security Finding Formats (ASFF) an Security Hub.

Hier ist ein Beispiel für ein typisches Ergebnis von GuardDuty.


```
  {
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws::securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
  "AwsAccountId": "193043430472",
  "Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
  ],
  "FirstObservedAt": "2020-08-22T09:15:57Z",
  "LastObservedAt": "2020-09-30T11:56:49Z",
  "CreatedAt": "2020-08-22T09:34:34.146Z",
  "UpdatedAt": "2020-09-30T12:14:00.206Z",
  "Severity": {
    "Product": 2,
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356.",
  "Description": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
 instance by guessing the SSH password.",
```

```
  "SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-
east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductFields": {
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
 "Unknown",
    "aws/guardduty/service/archived": "false",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lat": "42.5122",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4":
 "199.241.229.197",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lon": "-90.7384",
    "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port":
 "46717",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/
countryName": "United States",
    "aws/guardduty/service/serviceName": "guardduty",
    "aws/guardduty/service/evidence": "",
    "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4":
 "172.31.43.6",
    "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
org": "CenturyLink",
    "aws/guardduty/service/action/networkConnectionAction/connectionDirection":
 "INBOUND",
    "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
    "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName":
 "SSH",
    "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/
cityName": "Dubuque",
    "aws/guardduty/service/additionalInfo": "",
    "aws/guardduty/service/resourceRole": "TARGET",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
    "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",
    "aws/guardduty/service/count": "74",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asn": "209",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
isp": "CenturyLink",
```

```
    "aws/securityhub/FindingId": "arn:aws::securityhub:us-east-1::product/
aws/guardduty/arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
    "aws/securityhub/ProductName": "GuardDuty",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws::ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "Type": "t2.micro",
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "18.234.130.16",
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475",
          "LaunchedAt": "2020-08-03T23:21:57Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```


Aktivieren und Konfigurieren der Integration

Um die Integration mit verwenden zu können AWS Security Hub, müssen Sie Security Hub aktivieren. Informationen zur Aktivierung von Security Hub finden Sie unter Einrichten von Security Hub im AWS Security Hub -Leitfaden.

Wenn Sie GuardDuty sowohl als auch Security Hub aktivieren, wird die Integration automatisch aktiviert. GuardDutybeginnt sofort, Ergebnisse an Security Hub zu senden.

Einstellung der Veröffentlichung von Erkenntnissen in Security Hub

Um anzugeben, dass keine Erkenntnisse mehr an Security Hub gesendet werden, können Sie entweder die Security Hub-Konsole oder die API verwenden.

Weitere Informationen finden Sie unter Deaktivieren und Aktivieren des Ergebnisflusses aus einer Integration (Konsole) oder Deaktivieren des Ergebnisflusses aus einer Integration (Security Hub Hub-API, AWS CLI) im AWS Security Hub Benutzerhandbuch.

Integration mit Amazon Detective

Amazon Detective hilft Ihnen dabei, Sicherheitsereignisse in einem oder mehreren AWS-Konten schnell zu analysieren und zu untersuchen, indem es Datenvisualisierungen generiert, die das Verhalten und die Interaktion Ihrer Ressourcen im Laufe der Zeit darstellen. Detective erstellt Visualisierungen der Erkenntnisse von GuardDuty.

Detective nimmt Erkenntnisdetails für alle Erkenntnistypen auf und bietet Zugriff auf die Entitätsprofile, um verschiedene Entitäten zu untersuchen, die an der Erkenntnis beteiligt sind. Eine Entität kann ein AWS-Konto, eine AWS-Ressource innerhalb eines Kontos oder eine externe IP-Adresse sein, die mit Ihren Ressourcen interagiert hat. Die GuardDuty-Konsole unterstützt je nach Erkenntnistyp den Wechsel von den folgenden Entitäten zu Amazon Detective: AWS-Konto, IAM-Rolle, -Benutzer oder -Rollensitzung, Benutzeragent, Verbundbenutzer, Amazon-EC2-Instance oder IP-Adresse.

Inhalt

Aktivierung der Integration

Um Amazon Detective mit GuardDuty verwenden zu können, müssen Sie zuerst Amazon Detective aktivieren. Informationen zur Aktivierung von Detective finden Sie unter Amazon Detective einrichten in der Verwaltungsanleitung für Amazon Detective.

Wenn Sie sowohl GuardDuty als auch Security Hub aktivieren, wird die Integration automatisch aktiviert. Nach der Aktivierung nimmt Detective sofort Ihre GuardDuty-Erkenntnisdaten auf.

> **Note**
>
> GuardDuty sendet die Erkenntnisse auf der Grundlage der Exporthäufigkeit der GuardDuty-Erkenntnisse an Detective. Standardmäßig beträgt die Exporthäufigkeit für Aktualisierungen vorhandener Erkenntnisse 6 Stunden. Um sicherzustellen, dass Detective die neuesten Aktualisierungen Ihrer Ergebnisse erhält, wird empfohlen, die Exporthäufigkeit in jeder Region, in der Sie Detective mit GuardDuty verwenden, auf 15 Minuten zu ändern. Weitere Informationen finden Sie unter Schritt 5 — Einstellung der Häufigkeit für den Export aktualisierter aktiver Ergebnisse.

Von einer GuardDuty-Erkenntnis zu Amazon Detective wechseln

1. Melden Sie sich in der https://console.aws.amazon.com/guardduty/-Konsole an.
2. Wählen Sie eine einzelne Erkenntnis aus Ihrer Erkenntnistabelle aus.
3. Wählen Sie im Bereich mit den Erkenntnisdetails die Option Mit Detective untersuchen.
4. Wählen Sie einen Aspekt der Erkenntnis aus, den Sie mit Amazon Detective untersuchen möchten. Dadurch wird die Detective-Konsole für diese Erkenntnis oder diese Entität geöffnet.

Wenn sich der Wechsel nicht wie erwartet verhält, finden Sie weitere Informationen unter Fehlerbehebung beim Wechsel im Amazon-Detective-Benutzerhandbuch.

> **Note**
>
> Wenn Sie eine GuardDuty-Erkenntnis in der Detective-Konsole archivieren, wird diese Erkenntnis auch in der GuardDuty-Konsole archiviert.

Verwendung der Integration mit einer GuardDuty-Umgebung mit mehreren Konten

Wenn Sie in GuardDuty eine Umgebung mit mehreren Konten verwalten, müssen Sie Ihre Mitgliedskonten zu Amazon Detective hinzufügen, um Detective-Datenvisualisierungen für Erkenntnisse und Entitäten in diesen Konten zu sehen.

Es wird empfohlen, dasselbe GuardDuty-Administratorkonto wie das Administratorkonto für Detective zu verwenden. Weitere Informationen zum Hinzufügen von Mitgliedskonten in Detective finden Sie unter Mitgliedskonten einladen.

> **Note**
>
> Detective ist ein regionaler Service, d. h. Sie müssen Detective aktivieren und Ihre Mitgliedskonten in jeder Region hinzufügen, in der Sie die Integration verwenden möchten.

Aussetzen oder Deaktivieren GuardDuty

Sie können die GuardDuty Konsole verwenden, um den GuardDuty Service auszusetzen oder zu deaktivieren. Die Nutzung wird Ihnen nicht in Rechnung gestellt GuardDuty , wenn der Dienst gesperrt ist.

- Alle Mitgliedskonten müssen getrennt oder gelöscht werden, bevor Sie sie sperren oder deaktivieren GuardDuty können.
- Wenn Sie die GuardDuty Sperre sperren, wird die Sicherheit Ihrer AWS Umgebung nicht mehr überwacht und es werden keine neuen Erkenntnisse mehr generiert. Ihre vorhandenen Ergebnisse bleiben erhalten und sind von der GuardDuty Sperrung nicht betroffen. Sie können wählen, ob Sie es GuardDuty später wieder aktivieren möchten.
- Wenn Sie es GuardDuty in einem Konto deaktivieren, wird es nur für das aktuell ausgewählte AWS-Region Konto deaktiviert. Wenn Sie es vollständig deaktivieren möchten GuardDuty, müssen Sie es in jeder Region deaktivieren, in der es aktiviert ist.
- Wenn Sie die Option deaktivieren GuardDuty, gehen Ihre vorhandenen Ergebnisse und die GuardDuty Konfiguration verloren und können nicht wiederhergestellt werden. Wenn Sie Ihre vorhandenen Ergebnisse speichern möchten, müssen Sie sie exportieren, bevor Sie die Deaktivierung bestätigen GuardDuty. Weitere Informationen zum Exportieren von Erkenntnissen finden Sie unter Exportieren von Erkenntnissen.

Zum Sperren oder Deaktivieren GuardDuty

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie im GuardDuty Abschnitt „Sperren“ die Option „ GuardDutySperren“ oder „Deaktivieren GuardDuty“ und bestätigen Sie dann Ihre Aktion.

Um die Aktivierung nach GuardDuty dem Sperren wieder zu aktivieren

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie Erneut aktivieren. GuardDuty

Abonnieren von Amazon SNS GuardDuty -Ankündigungen

Dieser Abschnitt enthält Informationen zum Abonnieren von Amazon SNS (Simple Notification Service) für GuardDuty Ankündigungen, Benachrichtigungen über neu veröffentlichte Erkenntnistypen, Aktualisierungen der vorhandenen Erkenntnistypen und andere Funktionsänderungen zu erhalten. Benachrichtigungen sind in allen Formaten verfügbar, die Amazon SNS unterstützt.

Das GuardDuty SNS sendet Ankündigungen über Updates an den GuardDuty Service über AWS an jedes abonnierte Konto. Informationen, um Benachrichtigungen über Erkenntnisse in Ihrem Konto zu erhalten, finden Sie unter Erstellen von benutzerdefinierten Antworten auf GuardDuty Erkenntnisse mit Amazon CloudWatch Events.

> **Note**
>
> Ihr IAM-Benutzer muss `sns::subscribe`-Berechtigungen haben, ein SNS zu abonnieren.

Sie können eine Amazon SQS-Warteschlange für dieses Benachrichtigungsthema abonnieren, aber Sie müssen einen Themen-ARN verwenden, der sich in derselben Region befindet. Weitere Informationen finden Sie unter Tutorial: Abonnieren einer Amazon-SQS-Warteschlange zu einem Amazon-SNS-Thema im Entwicklerhandbuch für Amazon Simple Queue Service.

Sie können auch eine - AWS Lambda Funktion verwenden, um Ereignisse auszulösen, wenn Benachrichtigungen empfangen werden. Weitere Informationen finden Sie unter Aufrufen von Lambda-Funktionen mit Amazon-SNS-Benachrichtigungen im Enwicklerhandbuch für Amazon Simple Queue Service.

Die Amazon SNS-Thema-ARNs für jede Region sind unten aufgeführt.

AWS Region	ARN des Amazon-SNS-Themas
`us-east-1`	`arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements`

AWS Region	ARN des Amazon-SNS-Themas
us-east-2	arn:aws:sns:us-east-2:118283430703:GuardDutyAnnouncements
us-west-1	arn:aws:sns:us-west-1:144182107116:GuardDutyAnnouncements
us-west-2	arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements
ca-central-1	arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnouncements
ca-west-1	arn:aws:sns:ca-west-1:440427180217:GuardDutyAnnouncements
eu-north-1	arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnouncements
eu-west-1	arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnouncements

AWS Region	ARN des Amazon-SNS-Themas
eu-west-2	arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements
eu-west-3	arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements
eu-central-1	arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements
eu-central-2	arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements
ap-east-1	arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements
ap-northeast-1	arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements
ap-northeast-2	arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements

AWS Region	ARN des Amazon-SNS-Themas
ap-southeast-1	arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements
ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements
ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements
sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements
us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements
cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements
cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements

AWS Region	ARN des Amazon-SNS-Themas
me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements
me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements
eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements

AWS Region	ARN des Amazon-SNS-Themas
ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements
ap-southeast-4	arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements
il-central-1	arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements

So abonnieren Sie die GuardDuty Aktualisierungsbenachrichtigungs-E-Mail in der AWS Management Console

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie in der Regionsliste die gleiche Region aus, wie der Thema-ARN, den Sie abonnieren möchten. In diesem Beispiel wird die Region `us-west-2` verwendet.
3. Wählen Sie im linken Navigationsbereich Subscriptions (Abonnements) und danach Create subscription (Abonnement erstellen) aus.
4. Fügen Sie im Dialogfeld Create Subscription (Abonnement erstellen) unter Topic ARN (Themen-ARN) den Themen-ARN: `arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements` ein.
5. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus. Geben Sie unter Endpoint (Endpunkt) eine E-Mail-Adresse ein, um die Benachrichtigung zu empfangen.
6. Wählen Sie Create subscription (Abonnement erstellen) aus.
7. Öffnen Sie in Ihrer E-Mail-Anwendung die Nachricht unter AWS Benachrichtigungen und öffnen Sie den Link, um Ihr Abonnement zu bestätigen.

   Ihr Webbrowser zeigt eine Bestätigungsantwort vom Amazon SNS an.

So abonnieren Sie die GuardDuty Aktualisierungsbenachrichtigungs-E-Mail mit der AWS CLI

1. Führen Sie den folgenden Befehl mit der AWS CLIaus:

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. Öffnen Sie in Ihrer E-Mail-Anwendung die Nachricht unter AWS Benachrichtigungen und öffnen Sie den Link, um Ihr Abonnement zu bestätigen.

   Ihr Webbrowser zeigt eine Bestätigungsantwort vom Amazon SNS an.

Amazon-SNS-Nachrichtenformat

Im Folgenden wird ein Beispiel GuardDuty für eine Aktualisierungsbenachrichtigungsmeldung zu neuen Erkenntnissen gezeigt:

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FINDINGS\",\"findingDetails
\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"findingDescription\":\"This finding informs you that an EC2 instance in your AWS
 environment is making connections to a Tor Guard or an Authority node. Tor is software
 for enabling anonymous communication. Tor Guards and Authority nodes act as initial
 gateways into a Tor network. This traffic can indicate that this EC2 instance is
 acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised.\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
```

```
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

Die geparste Benachrichtigung (mit entfernten Escape-Zeichen) ist nachfolgend gezeigt:

```
{
    "version": "1",
    "type": "NEW_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "findingDescription": "This finding informs you that an EC2 instance in your
 AWS environment is making connections to a Tor Guard or an Authority node. Tor is
 software for enabling anonymous communication. Tor Guards and Authority nodes act as
 initial gateways into a Tor network. This traffic can indicate that this EC2 instance
 is acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised."
    }]
}
```

Ein Beispiel GuardDuty für eine Aktualisierungsbenachrichtigung über GuardDuty Funktionsaktualisierungen wird unten gezeigt:

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FEATURES\",\"featureDetails
\":[{\"featureDescription\":\"Customers with high-volumes of global CloudTrail
 events should see a net positive impact on their GuardDuty costs.\",\"featureLink
\":\"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_data-
sources.html#guardduty_cloudtrail\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
```

```
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

Die geparste Benachrichtigung (mit entfernten Escape-Zeichen) ist nachfolgend gezeigt:

```
{
    "version": "1",
    "type": "NEW_FEATURES",
    "featureDetails": [{
        "featureDescription": "Customers with high-volumes of global CloudTrail events
 should see a net positive impact on their GuardDuty costs.",
        "featureLink": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_data-sources.html#guardduty_cloudtrail"
    }]
}
```

Ein Beispiel GuardDuty für eine Aktualisierungsbenachrichtigungsmeldung zu aktualisierten Ergebnissen ist unten dargestellt:

```
{
    "Type": "Notification",
    "MessageId": "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn": "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message": "{\"version\":\"1\",\"type\":\"UPDATED_FINDINGS\",
\"findingDetails\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"description\":\"Increased severity value from 5 to 8.\"}]}",
    "Timestamp": "2018-03-09T00:25:43.483Z",
    "SignatureVersion": "1",
    "Signature": "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
```

```
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

Die geparste Benachrichtigung (mit entfernten Escape-Zeichen) ist nachfolgend gezeigt:

```
{
    "version": "1",
    "type": "UPDATED_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "description": "Increased severity value from 5 to 8."
    }]
}
```

Kontingente für Amazon GuardDuty

Ihr AWS Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden AWS Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Für einige Kontingente können Sie Erhöhungen beantragen, während andere Kontingente nicht erhöht werden können.

Um die Kontingente für anzuzeigen GuardDuty, öffnen Sie die Konsole Service Quotas. Wählen Sie im Navigationsbereich AWS Services und dann Amazon aus GuardDuty.

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Ihr AWS Konto hat die folgenden Kontingente für Amazon GuardDuty pro Region.

> **Note**
>
> Spezifische Kontingente für den GuardDuty Malware-Schutz finden Sie unterKontingente für Malware Protection.

Ressource	Standard	Kommentare
Detektoren	1	Die maximale Anzahl an Detektorr essourcen, die Sie pro AWS -Konto und Region erstellen können. Sie können keine Erhöhung des Kontingents beantragen.
Filter	100	Die maximale Anzahl an gespeicherten

Ressource	Standard	Kommentare
		Filtern pro AWS Konto und Region. Sie können keine Erhöhung des Kontingents beantragen.
Aufbewahrungszeitraum für Ergebnisse	90 Tage	Die maximale Anzahl von Tagen, die ein Ergebnis aufbewahrt wird. Sie können keine Erhöhung des Kontingents beantragen.
IP-Adressen und CIDR-Bereiche pro Liste vertrauenswürdiger IPs	2.000	Die maximale Anzahl von IP-Adressen und CIDR-Bereichen, die Sie in eine einzelne Liste vertrauenswürdiger IPs aufnehmen können. Sie können keine Erhöhung des Kontingents beantragen.

Ressource	Standard	Kommentare
IP-Adressen und CIDR-Bereiche pro Bedrohungsliste	250 000	Die maximale Anzahl von IP-Adress- und CIDR-Bereichen, die Sie in eine Bedrohungsliste aufnehmen können. Sie können keine Erhöhung des Kontingents beantragen.
Maximale Dateigröße	35 MB	Die maximale Größe für die Datei, die verwendet wird, um eine Liste von IP-Adressen oder CIDR-Bereichen hochzuladen, die in eine Liste vertrauenswürdiger IPs oder Bedrohungsliste aufgenommen werden sollen. Sie können keine Erhöhung des Kontingents beantragen.

Ressource	Standard	Kommentare
Mitgliedskonten (nach Einladung)	5000	Die maximale Anzahl von Mitgliedskonten, die einem Administr atorkonto zugeordnet sind. Sie können keine Erhöhung des Kontingents beantragen.

Ressource	Standard	Kommentare
Mitgliedskonten	50 000	Die maximale Anzahl von Mitgliedskonten, die einem Administratorkonto zugeordnet sind AWS Organizations. Dazu gehören auch Mitgliedskonten, die der Organisation auf Einladung hinzugefügt werden. Dieser Standardwert hängt von Ihrem aktuellen Kontingent für Mitgliedskonten in ab AWS Organizations. Die Anzahl der Mitgliedskonten GuardDuty , über AWS Organizations die hinzugefügt werden, darf die Anzahl der Mitgliedskonten in Ihrer Organisation nicht überschreiten. Informationen zur Anzahl von AWS-Konten in einer Organisation finden Sie unter Höchst- und Mindestwerte im AWS Organizations Benutzerhandbuch.

Ressource	Standard	Kommentare
Threat-Intelligence-Sätze	6	Die maximale Anzahl von Threat-Intelligence-Sätzen, die Sie pro AWS -Konto und Region hinzufügen können. Sie können keine Erhöhung des Kontingents beantragen.
Vertrauenswürdige IP-Sätze	1	Die maximale Anzahl vertrauenswürdiger IP-Sets, die pro AWS Konto und Region hochgeladen und aktiviert werden können. Sie können keine Erhöhung des Kontingents beantragen.

Problembehebung bei Amazon GuardDuty

Wenn Sie Probleme im Zusammenhang mit der Durchführung einer bestimmten Aktion von haben GuardDuty, lesen Sie die Themen in diesem Abschnitt.

Themen

Allgemeine Probleme in GuardDuty

Ich erhalte beim Exportieren der GuardDuty Ergebnisse einen Zugriffsfehler. Wie kann ich dieses Problem lösen?

Wenn GuardDuty Sie die Einstellungen für den Export von Ergebnissen konfiguriert haben und die Ergebnisse nicht exportiert werden können, wird auf der Seite Einstellungen in der GuardDuty Konsole eine Fehlermeldung angezeigt. Dies kann möglicherweise passieren, wenn GuardDuty Sie nicht mehr auf die Zielressource zugreifen können, z. B. wenn Ihr Amazon S3 S3-Bucket gelöscht oder die Zugriffsberechtigung für den Bucket geändert wurde. Dies kann möglicherweise auch passieren, wenn GuardDuty Sie nicht mehr auf den AWS KMS Schlüssel zugreifen können, der zur Verschlüsselung der Daten in Ihrem Amazon S3 S3-Bucket verwendet wurde. Wenn der Export nicht möglich GuardDuty ist, sendet es eine Benachrichtigung an die mit dem Konto verknüpfte E-Mail-Adresse mit Informationen zu diesem Problem.

Um das Problem zu lösen, stellen Sie sicher, dass die entsprechenden Ressourcen vorhanden sind und GuardDuty über die erforderlichen Zugriffsrechte verfügen. Wenn Sie das Problem nicht vor Ablauf der 90-tägigen Aufbewahrungsfrist für Ergebnisse lösen GuardDuty, werden Ihre Ergebnisse nicht exportiert. GuardDuty deaktiviert die Suche nach Exporteinstellungen für dieses Konto in der jeweiligen Region. Auch nach Ablauf dieses Aufbewahrungsdatums können Sie die Konfigurationseinstellungen aktualisieren, um den Export der Ergebnisse in der jeweiligen Region wieder aufzunehmen.

Weitere Informationen finden Sie unter Exportieren von Erkenntnissen.

Probleme beim Schutz vor Schadsoftware

Ich initiiere einen Malware-Scan auf Abruf, der jedoch zu einem Fehler wegen fehlender erforderlicher Berechtigungen führt.

Wenn Sie eine Fehlermeldung erhalten, die darauf hindeutet, dass Sie nicht über die erforderlichen Berechtigungen verfügen, um einen Malware-Scan auf Abruf auf einer Amazon-EC2-Instance zu starten, überprüfen Sie, ob Sie Ihrer IAM-Rolle die AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess-Richtlinie angefügt haben.

Wenn Sie Mitglied einer AWS Organisation sind und immer noch dieselbe Fehlermeldung erhalten, stellen Sie eine Verbindung mit Ihrem Verwaltungskonto her. Weitere Informationen finden Sie unter AWS Organizations SCP — Zugriff verweigert.

Ich erhalte bei der Arbeit mit Malware Protection eine **`iam:GetRole`**-Fehlermeldung.

Wenn Sie die folgende Fehlermeldung erhalten —`Unable to get role: AWSServiceRoleForAmazonGuardDutyMalwareProtection`, bedeutet das, dass Sie nicht berechtigt sind, entweder den von Ihnen GuardDuty initiierten Malware-Scan zu aktivieren oder den On-Demand-Malware-Scan zu verwenden. Stellen Sie sicher, dass Sie die AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess-Richtlinie Ihrer IAM-Rolle angehängt haben.

Ich habe ein GuardDuty Administratorkonto und muss den GuardDuty -initiierten Malware-Scan aktivieren, verwende aber keine AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess zur Verwaltung. GuardDuty

- Konfigurieren Sie die IAM-Rolle, die Sie mit verwenden, so, dass Sie über die erforderlichen Berechtigungen verfügen, GuardDuty um den GuardDuty -initiierten Malware-Scan zu aktivieren. Weitere Informationen zu den erforderlichen Berechtigungen finden Sie unter Eine serviceverknüpfte Rolle für Malware Protection erstellen.
- Fügen Sie die AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess an Ihre IAM-Rolle an. Auf diese Weise können Sie den GuardDuty -initiierten Malware-Scan für die Mitgliedskonten aktivieren.

Probleme mit der Laufzeitüberwachung

Mein AWS Step Functions Workflow schlägt unerwartet fehl

Wenn der GuardDuty Container zum Workflow-Fehler beigetragen hat, finden Sie weitere Informationen unterFehlerbehebung bei Abdeckungsproblemen. Wenn das Problem weiterhin besteht, führen Sie einen der folgenden Schritte aus, um zu verhindern, dass der Workflow aufgrund des GuardDuty Containers fehlschlägt:

- Fügen Sie das `false` Tag`GuardDutyManaged`: zum zugehörigen Amazon ECS-Cluster hinzu.
- Deaktivieren Sie die automatische Agentenkonfiguration für AWS Fargate (nur ECS) auf Kontoebene. Fügen Sie das Inclusion-Tag`GuardDutyManaged`: `true` zu dem zugehörigen Amazon ECS-Cluster hinzu, den Sie mit dem GuardDuty automatisierten Agenten weiter überwachen möchten.

Fehlerbehebung bei Speichermangel in Runtime Monitoring (nur Amazon EC2-Support)

In diesem Abschnitt werden die Schritte zur Problembehebung beschrieben, wenn der Fehler „Nicht genügend Arbeitsspeicher“ auftritt, basierend auf dem Problem, den GuardDuty Security Agent manuell CPU- und Speicherlimit zu installieren.

Wenn der GuardDuty Agent aufgrund des `out-of-memory` Problems `systemd` beendet wird und Sie der Meinung sind, dass es sinnvoll ist, dem GuardDuty Agenten mehr Speicher zur Verfügung zu stellen, können Sie das Limit aktualisieren.

1. Öffnen `/lib/systemd/system/amazon-guardduty-agent.service` Sie mit der Root-Berechtigung.
2. Suchen Sie `MemoryLimit` nach und und aktualisieren Sie beide Werte. `MemoryMax`

```
MemoryLimit=256MB
MemoryMax=256MB
```

3. Starten Sie den GuardDuty Agenten nach dem Aktualisieren der Werte neu, indem Sie den folgenden Befehl verwenden:

```
sudo systemctl daemon-reload
```

```
sudo systemctl restart amazon-guardduty-agent
```

4. Führen Sie den folgenden Befehl aus, um den Status anzuzeigen:

```
sudo systemctl status amazon-guardduty-agent
```

In der erwarteten Ausgabe wird das neue Speicherlimit angezeigt:

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

Probleme mit der Verwaltung mehrerer Konten

Ich möchte mehrere Konten verwalten, benötige aber keine AWS Organizations Verwaltungsberechtigung.

Wenn Sie diese Fehlermeldung erhalten —`The request failed because you do not have required AWS Organization master permission.`, bedeutet das, dass Sie nicht berechtigt sind, den GuardDuty -initiierten Malware-Scan für mehrere Konten in Ihrer Organisation zu aktivieren. Weitere Informationen zur Erteilung von Berechtigungen für das Verwaltungskonto finden Sie unterEinrichtung eines vertrauenswürdigen Zugriffs zur Aktivierung des GuardDuty -initiierten Malware-Scans.

Fehlerbehebung bei anderen Problemen

Wenn Sie kein geeignetes Szenario für Ihr Problem finden, sehen Sie sich die folgenden Optionen zur Fehlerbehebung an:

- Informationen zu allgemeinen IAM-Problemen beim Zugriff auf https://console.aws.amazon.com/guardduty/ finden Sie unter Fehlerbehebung Amazon GuardDuty Amazon-Identität und -Zugriff.
- Informationen zu Authentifizierungs- und Autorisierungsproblemen beim Zugriff AWS AWS Console Home finden Sie unter Problembehandlung bei IAM.

Regionen und Endpunkte

Informationen darüber, AWS-Regionen wo Amazon verfügbar GuardDuty ist, finden Sie unter GuardDuty Amazon-Endpunkte in der Allgemeine Amazon Web Services-Referenz.

Wir empfehlen Ihnen, alle unterstützten GuardDuty AWS-Regionen Optionen zu aktivieren. Auf diese Weise können GuardDuty auch in Regionen, die Sie nicht aktiv nutzen, Erkenntnisse über unbefugte oder ungewöhnliche Aktivitäten generiert werden. Auf diese Weise können GuardDuty auch AWS CloudTrail Ereignisse für die unterstützten Länder überwacht werden. Die Fähigkeit AWS-Regionen, Aktivitäten zu erkennen, die globale Dienste betreffen, ist eingeschränkt.

Verfügbarkeit regionsspezifischer Feature

Eine Liste mit regionalen Unterschieden, um die Verfügbarkeit von GuardDuty Funktionen zu spezifizieren.

ListFindings und GetFindingsStatistics APIs

Die ListFindingsAPIs GetFindingsStatisticsund haben ein temporäres `consoleOnly` Flag. Wenn Sie eine oder beide dieser APIs verwenden, bedeutet das `consoleOnly` Flag, dass die API Ergebnisse bis zu einer Höchstgrenze von 1000 abrufen kann.

GuardDuty Funktionen mit regionalen Unterschieden

GuardDuty Schutz vor Schadsoftware

GuardDuty unterstützt die Malware-Schutzfunktion in den AWS Dedicated Local Zones.

Die folgenden APIs in der Amazon GuardDuty API-Referenz können regionale Unterschiede aufweisen, da einige der zuvor angegebenen AWS-Regionen Datenquellen oder Funktionen nicht verfügbar sind:

- CreateDetector
- UpdateDetector
- UpdateMemberDetectors
- UpdateOrganizationConfiguration
- GetDetector
- GetMemberDetectors
- DescribeOrganizationConfiguration

Amazon-EC2-Erkenntnistypen – DefenseEvasion:EC2/UnusualDoHActivity und DefenseEvasion:EC2/UnusualDoTActivity

Die folgende Tabelle zeigt, AWS-Regionen wo verfügbar GuardDuty ist, aber diese beiden Amazon EC2-Suchttypen werden noch nicht unterstützt.

AWS-Region	Regionscode
Asien-Pazifik (Seoul)	ap-northeast-2
Asien-Pazifik (Osaka)	ap-northeast-3
Asien-Pazifik (Jakarta)	ap-southeast-3

AWS GovCloud (US) Regionen

Aktuelle Informationen finden Sie unter Amazon GuardDuty im AWS GovCloud (US) Benutzerhandbuch.

Regionen in China

Aktuelle Informationen finden Sie unter Verfügbarkeit von Features und Unterschiede bei der Implementierung.

GuardDuty Legacy-Aktionen und -Parameter

Amazon GuardDuty hat einige der API-Aktionen und -Parameter als veraltet eingestuft, unterstützt sie aber weiterhin. Es hat sich bewährt, die neuen API-Aktionen und -Parameter zu verwenden, die die alten Optionen ersetzen. Die folgende Tabelle vergleicht die alten und neuen Aktionen und Parameter.

Ältere Aktionen/ Parameter	Ältere Aktionen/Parameter	Vergleich
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	Mit derselben Implementierung in beiden Aktionen GuardDuty verwendet den Begriff `Administrator` in `DisassociateFromAdministratorAccount` .
`autoEnable` -Parameter in DescribeOrganizationConfiguration und UpdateOrganizationConfiguration	`autoEnableOrganizationMembers`	Mit kann `autoEnableOrganizationMembers` das GuardDuty Administratorkonto GuardDuty für alle Mitgliedskonten einen der Werte prüfen und durchsetzen. Bei der Verwendung von APIs kann die Aktualisierung der Konfiguration aller Mitgliedskonten bis zu 24 Stunden dauern. Weitere Informationen zu den möglichen Werten des `autoEnableOrganizationMembers` Felds finden Sie unter autoEnableOrganizationMitglieder
`dataSources` -Parameter in den APIs, die in GuardDuty API-Änderungen	`features`	Ab März 2023 können Sie Malware-Schutz bei Amazon GuardDuty und die neuen GuardDuty Schutzpläne mit konfigurieren`features`. Die vor März 2023 eingeführten Schutzpläne, einschließlich Malware Protection,

Ältere Aktionen/ Parameter	Ältere Aktionen/Parameter	Vergleich
im März 2023 aufgeführt sind.		unterstützen weiterhin die Konfigura tion mit `dataSources` . Wenn Sie APIs verwenden, um einen Schutzpla n zu konfigurieren, kann jede API-Anfrage entweder `dataSources` oder `features` beinhalten, aber nicht beide.

Dokumentenverlauf für Amazon GuardDuty

In der folgenden Tabelle werden wichtige Änderungen an der Dokumentation seit der letzten Version des GuardDuty Amazon-Benutzerhandbuchs beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Aktualisierte Funktionalität in GuardDuty Runtime Monitoring — Fargate (nur Amazon ECS)	Runtime Monitoring hat eine neue Agentenversion 1.2.0 für Ressourcen AWS Fargate (nur Amazon ECS) veröffentlicht. Weitere Informationen zu den Versionshinweisen finden Sie unter GuardDuty Security Agent for Fargate-ECS.	31. Mai 2024
Die Funktionalität des GuardDuty Malware-Schutzes wurde aktualisiert	Für jedes Amazon EBS-Volume, das an Ihre Amazon EC2 EC2-Instances und Container-Workloads angehängt ist, hat GuardDuty Malware Protection die Größe des EBS-Volumes, das gescannt wird, auf bis zu 2048 GB erhöht. Informationen zum Scannen von Amazon EBS-Volumes, die an Ihre Instances angehängt sind, finden Sie unter GuardDuty Malware-Schutz.	29. Mai 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring für Amazon ECS-Fargate-Ressourcen unterstützt jetzt die Erkennung potenzieller Bedrohungen für Ihre Aufgaben, die von gestartet	28. Mai 2024

	wurden. AWS Batch Weitere Informationen finden Sie unter So funktioniert Runtime Monitoring with Fargate (nur Amazon ECS).	
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat eine neue Agentenversion 1.6.1 für Amazon EKS-Ressourcen veröffentlicht. Informationen zu Versionshinweisen finden Sie in der Versionsgeschichte des EKS-Add-On-Agenten.	14. Mai 2024
Erweiterte Regionsunterstützung für Runtime Monitoring	GuardDuty erweitert die Unterstützung für Runtime Monitoring auf die Region Canada West (Calgary) . Informationen zu den ersten Schritten mit Runtime Monitoring finden Sie unter Runtime Monitoring aktivieren.	7. Mai 2024

Erweiterte regionale Unterstützung für RDS Protection	GuardDuty erweitert die Unterstützung von RDS Protection auf Folgendes AWS-Regionen: • Kanada West (Calgary) • Asien-Pazifik (Hyderabad) • Europa (Spain) • Europa (Zürich) • Naher Osten (VAE) • Israel (Tel Aviv) • Asien-Pazifik (Melbourne) Informationen zur Aktivierung dieser Funktion finden Sie unter RDS-Schutz.	3. Mai 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat eine neue Agentenversion 1.1.0 für Ressourcen AWS Fargate (nur Amazon ECS) veröffentlicht. Weitere Informationen zu den Versionshinweisen finden Sie unter GuardDuty Security Agent for Fargate-ECS.	1. Mai 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat eine neue Agentenversion 1.6.0 für Amazon EKS-Ressourcen veröffentlicht. Informationen zu Versionshinweisen finden Sie in der Versionsgeschichte des EKS-Add-On-Agenten.	29. April 2024

Support für IPAddressV6	GuardDuty hat IPAddressV6-Unterstützung für lokale und Remote-IP-Details hinzugefügt. Sie können die zugehörigen Filterattribute verwenden, um GuardDuty Ergebnisse zu filtern oder Unterdrückungsregeln zu erstellen.	18. April 2024
Die Konsolenoberfläche wurde aktualisiert, um den Export von Ergebnissen zu konfigurieren	GuardDuty hat die Konsolenoberfläche aktualisiert, sodass die in Ihrem AWS-Konten generierten Ergebnisse in einen Amazon S3 S3-Bucket exportiert werden. Weitere Informationen finden Sie unter GuardDuty Ergebnisse exportieren.	1. April 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat einen neuen Security Agent Version 1.1.0 für die Amazon EC2 EC2-Ressource veröffentlicht. Diese Version unterstützt die GuardDuty automatische Agentenkonfiguration in Runtime Monitoring für Amazon EC2 EC2-Instances. Informationen zu Versionshinweisen finden Sie unter GuardDuty Security Agent für Amazon EC2 EC2-Instance.	28. März 2024

Allgemeine Verfügbarkeit von Runtime Monitoring für Amazon EC2 EC2-Instances	GuardDuty kündigt die allgemeine Verfügbarkeit (GA) von Runtime Monitoring für Amazon EC2 EC2-Instances an. Jetzt haben Sie die Möglichkeit, die automatische Agentenkonfiguration zu aktivieren, mit der Sie GuardDuty den Security Agent für Ihre Amazon EC2 EC2-Instances in Ihrem Namen installieren und verwalten können. Mit dem GuardDuty automatisierten Agenten können Sie auch Inklusions- oder Ausschluss-Tags verwenden, um Sie darüber GuardDuty zu informieren, dass der Security Agent nur auf ausgewählten Amazon EC2 EC2-Instances installiert und verwaltet werden soll. Weitere Informationen finden Sie unter So funktioniert Runtime Monitoring mit Amazon EC2 EC2-Instances. Liste der neuen Findetypen, die zusammen mit dieser GA veröffentlicht wurden • Ausführung: Runtime/SuspiciousTool • Ausführung: Runtime/SuspiciousCommand	28. März 2024

- DefenseEvasionAusführung: Runtime/ ----SEP----:Runtime/ SuspiciousCommand
- DefenseEvasion:Runtime/ ----SEP----:Runtime/ PtraceAntiDebugging
- Ausführung: Runtime/ MaliciousFileExecuted

Amazon GuardDuty hat die serviceverknüpfte Rolle (SLR) aktualisiert	Verwenden Sie AWS Systems Manager Aktionen, um SSM-Verknüpfungen auf Amazon EC2-Instances zu verwalten, wenn Sie GuardDuty Runtime Monitoring mit automatisiertem Agenten für Amazon EC2 aktivieren. Wenn die GuardDuty automatische Agentenkonfiguration deaktiviert ist, werden nur die EC2-Instances GuardDuty berücksichtigt, die über ein Inclusion-Tag (:) verfügen. `GuardDutyManaged true` • Die folgende Liste zeigt die neuen Berechtigungen: `"ssm:DescribeAssociation", "ssm:DeleteAssociation", "ssm:UpdateAssociation", "ssm:CreateAssociation", "ssm:StartAssociationsOnce", "ssm:AddTagsToResource", "ssm:CreateAssociation", "ssm:UpdateAssociation", "ssm:SendCommand", "ssm:GetCommandInvocation"`	26. März 2024

Die Funktionalität in Runtime Monitoring wurde aktualisiert	Mit der neuesten Version des GuardDuty Security Agents (Add-on) v1.5.0 für Amazon EKS unterstützt Runtime Monitoring jetzt die Konfiguration bestimmter Parameter Ihres GuardDuty Security Agents, wie CPU- und Speichereinstellungen, `PriorityClass` Einstellungen und DNS-Richtlinieneinstellungen. Weitere Informationen finden Sie unter Konfiguration der Parameter des GuardDuty Security Agents (EKS-Add-on).	7. März 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat eine neue Agentenversion 1.5.0 für Amazon EKS-Ressourcen veröffentlicht. Informationen zu Versionshinweisen finden Sie in der Versionsgeschichte des EKS-Add-On-Agenten.	7. März 2024
Support für Canada West (Calgary)	Amazon GuardDuty ist jetzt in der Region Kanada West (Calgary) verfügbar. Einige der darin enthaltenen Schutzpläne sind in dieser Region GuardDuty möglicherweise nicht verfügbar. Die neuesten Informationen finden Sie unter Regionen und Endpunkte.	6. März 2024

Die Funktionalität in Runtime Monitoring wurde aktualisiert	Die GuardDuty Security Agent-Versionen 1.0.0 und 1.1.0 für Amazon EKS-Cluster werden ab dem 14. Mai 2024 nicht mehr unterstützt. Informationen darüber, welche Schritte Sie vor Ablauf des Standardsupports ergreifen können, finden Sie unter GuardDuty Sicherheitsagent für Amazon EKS-Cluster.	16. Februar 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring unterstützt die neueste Kubernetes-Version 1.29 mit der vorhandenen Security Agent-Version 1.4.1. Die Unterstützung ist seit dem Start dieser Kubernetes-Version verfügbar. Informationen zu den unterstützten Kubernetes-Versionen finden Sie unter Vom Security Agent unterstützte Kubernetes-Versionen. GuardDuty	16. Februar 2024

Aktualisierte Funktionalität in Runtime Monitoring — Regionale Verfügbarkeit	GuardDuty Runtime Monitoring unterstützt jetzt gemeinsam genutzte Amazon VPC innerhalb derselben AWS Organizations. GuardDuty Die serviceverknüpfte Rolle (SLR) verfügt über eine neue Berechtigung, mit der `organizations:DescribeOrganization` die Organisations-ID für das gemeinsam genutzte Amazon VPC-Konto abgerufen werden kann, um die Endpunktrichtlinie festzulegen. Informationen zu den Voraussetzungen für die Verwendung eines gemeinsam genutzten Amazon VPC-Endpunkts in Runtime Monitoring finden Sie unter Support für gemeinsam genutzte Amazon VPC. Diese Funktion ist in allen Regionen verfügbar, in denen Runtime Monitoring GuardDuty unterstützt wird.	12. Februar 2024

Aktualisierte Funktionalität in Runtime Monitoring — Regionale Verfügbarkeit	GuardDuty Runtime Monitoring unterstützt jetzt gemeinsam genutzte Amazon VPC innerhalb derselben AWS Organizations. GuardDuty Die serviceverknüpfte Rolle (SLR) verfügt über eine neue Berechtigung, mit der `organizations:DescribeOrganization` die Organisations-ID für das gemeinsam genutzte Amazon VPC-Konto abgerufen werden kann, um die Endpunktrichtlinie festzulegen. Informationen zu den Voraussetzungen für die Verwendung eines gemeinsam genutzten Amazon VPC-Endpunkts in Runtime Monitoring finden Sie unter Support für gemeinsam genutzte Amazon VPC. Derzeit ist diese Funktion in einigen der verfügbar . AWS-Regionen Weitere Informationen finden Sie unter Regionen und Endpunkte.	9. Februar 2024
Aktualisierte Funktionalität mit Unterstützung für den AWS-Regionen neuen Malware-Schutz	Der Malware-Schutz unterstützt jetzt das Scannen von EBS-Volumes, mit denen Von AWS verwaltete Schlüssel in der Region USA West (Oregon) verschlüsselt wurde.	6. Februar 2024

Aktualisierte Funktionalität mit Unterstützung für den AWS-Regionen neuen Malware-Schutz	Der Malware-Schutz unterstützt jetzt das Scannen von EBS-Volumes, die wie folgt AWS-Regionen verschlüsselt sind: Von AWS verwaltete Schlüssel • Asien-Pazifik (Singapur) (`ap-southeast-1`) • Europa (Frankfurt) (`eu-central-1`) • Asien-Pazifik (Osaka) (`ap-northeast-3`) • USA Ost (Ohio) (`us-east-2`) • Europa (Mailand) (`eu-south-1`) • Asien-Pazifik (Tokio) (`ap-northeast-1`) • Asien-Pazifik (Seoul) (`ap-northeast-2`) • Kanada (Zentral) (`ca-central-1`) • Europa (Irland) (`eu-west-1`) • USA Ost (Nord-Virginia) (`us-east-1`)	5. Februar 2024

Die Funktionalität in Runtime Monitoring wurde aktualisiert	GuardDuty Runtime Monitoring hat eine neue Version des GuardDuty Security Agents (v1.0.2) für Amazon EC2 EC2-Instances veröffentlicht. Diese Agentenversion beinhaltet Unterstützung für die neuesten Amazon ECS-AMIs. Weitere Informationen zum Versionsverlauf von Agenten finden Sie unter GuardDuty Sicherheitsagent für Amazon EC2 EC2-Instances.	2. Februar 2024

Aktualisierte Funktionalität mit Unterstützung für den AWS-Regionen neuen Malware-Schutz	Malware Protection unterstützt jetzt das Scannen der Amazon EBS-Volumes, die wie folgt AWS-Regionen verschlüsselt sind: Von AWS verwaltete Schlüssel • Europa (London) (`eu-west-2`) • Europa (Stockholm) (`eu-north-1`) • Asien-Pazifik (Hongkong) (`ap-east-1`) • Afrika (Kapstadt) (`af-south-1`) • Naher Osten (Bahrain) (`me-south-1`) • Asien-Pazifik (Hyderabad) (`ap-south-2`) • Europa (Spanien) (`eu-south-2`) • Asien-Pazifik (Melbourne) (`ap-southeast-4`) • Asien-Pazifik (Sydney) (`ap-southeast-2`) • Israel (Tel Aviv) (`il-central-1`)	31. Januar 2024

Die Verwaltung von Konten wurde aktualisiert mit AWS Organizations	Der Inhalt unter Konten verwalten mit AWS Organizations wurde neu organisiert. , fügte Schritte zum Ändern des delegierten GuardDuty Administratorkontos hinzu und aktualisierte Informationen zur Beziehung zwischen GuardDuty Administratorkonto und Mitgliedskonten.	30. Januar 2024
Aktualisierte Funktionalität mit Unterstützung für neue AWS-Regionen	Der Malware-Schutz unterstützt jetzt das Scannen von EBS-Volumes, die wie folgt AWS-Regionen verschlüsselt sind: Von AWS verwaltete Schlüssel • Asien-Pazifik (Jakarta) (`ap-southeast-3`) • USA West (Nordkalifornien) (`us-west-1`) • Naher Osten (VAE) (`me-central-1`) • Europa (Zürich) (`eu-central-2`) • Asien-Pazifik (Mumbai) (`ap-south-1`) • Südamerika (São Paulo) (`sa-east-1`)	29. Januar 2024

Die Funktionalität des Malware-Schutzes wurde aktualisiert	Der Malware-Schutz unterstützt jetzt das Scannen von EBS-Volumes, die mit Von AWS verwaltete Schlüssel verschlüsselt wurden. Die serviceverknüpfte Rolle (SLR) für den Malware-Schutz verfügt über zwei neue Berechtigungen — und. `GetSnapshotBlock` `ListSnapshotBlocks` Diese Berechtigungen helfen dabei, den Snapshot eines EBS-Volumes (verschlüsselt mit Von AWS verwalteter Schlüssel) von Ihrem GuardDuty abzurufen AWS-Konto und in das GuardDuty Dienstkonto zu kopieren, bevor der Malware-Scan gestartet wird. Derzeit ist diese Funktion nur in Europa (Paris) (`eu-west-3`) verfügbar . Weitere Informationen finden Sie unter Unterstützte Volumes für den Malware-Scan.	25. Januar 2024

Die Funktionalität in Runtime Monitoring wurde aktualisiert	GuardDuty Runtime Monitoring hat eine neue Version des GuardDuty Security Agents (v1.0.1) mit allgemeiner Leistungsoptimierung und Verbesserungen veröffentlicht. Weitere Informationen zum Versionsverlauf von Agenten finden Sie unter GuardDuty Sicherheitsagent für Amazon EC2 EC2-Instances.	23. Januar 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat eine neue Agentenversion 1.4.1 für Amazon EKS-Ressourcen veröffentlicht. Weitere Informationen finden Sie in der Versionshistorie des EKS-Add-On-Agenten.	16. Januar 2024
Runtime Monitoring hat den neuen Agenten v1.4.0 für Amazon EKS-Ressourcen veröffentlicht	Runtime Monitoring hat eine neue Agentenversion 1.4.0 für Amazon EKS-Ressourcen veröffentlicht. Weitere Informationen finden Sie in der Versionshistorie des EKS-Add-On-Agenten.	21. Dezember 2023

In Europa (Zürich), Europa (Spanien), Asien-Pazifik (Hyderabad), Asien-Pazifik (Melbourne) und Israel (Tel Aviv) wurden die Befundtypen S3 und AWS CloudTrail maschinelles Lernen (ML) hinzugefügt	Die folgenden S3 und CloudTrail Ergebnisse, die das anomale Verhalten mithilfe GuardDuty des ML-Modells zur Erkennung von Anomalien identifizieren, sind jetzt in den Regionen Europa (Zürich), Europa (Spanien), Asien-Pazifik (Hyderabad), Asien-Pazifik (Melbourne) und Israel (Tel Aviv) verfügbar: • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior • Persistence:IAMUser/AnomalousBehavior	21. Dezember 2023

	• PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty unterstützt 50.000 Mitgliedskonten durch AWS Organizations	Ein delegierter GuardDuty Administrator kann jetzt maximal 50.000 Mitglieds konten über AWS Organizat ions verwalten. Dazu gehören auch maximal 5000 Mitglieds konten, die dem GuardDuty Administratorkonto auf Einladung zugeordnet wurden.	20. Dezember 2023
GuardDuty Die Unterstützung für Runtime Monitoring wurde auf 19 erweitert AWS-Regio nen	Runtime Monitoring ist jetzt in Asien-Pazifik (Jakarta), Europa (Paris), Asien-Pazifik (Osaka), Asien-Pazifik (Seoul), Naher Osten (Bahrain), Europa (Spanien), Asien-Paz ifik (Hyderabad), Asien-Paz ifik (Melbourne), Israel (Tel Aviv), USA West (Nordkali fornien), Europa (London), Asien-Pazifik (Hongkong), Europa (Mailand), Naher Osten (VAE), Südamerika (São Paulo) verfügbar), Asien-Pazifik (Mumbai), Kanada (Zentral), Afrika (Kapstadt), Europa (Zürich).	6. Dezember 2023

GuardDuty erweitert die Funktionen zur Runtime-Überwachung	GuardDuty Kündigt neben der Erkennung von Bedrohungen für Ihre Amazon EKS-Cluster die allgemeine Verfügbarkeit von Runtime Monitoring zur Erkennung von Bedrohungen für Ihre Amazon ECS-Workloads und eine Vorabversion zur Erkennung von Bedrohungen für Ihre Amazon EC2 EC2-Instances an. Weitere Informationen darüber, welche AWS-Regionen derzeit Runtime Monitoring unterstützen, finden Sie unter Regionen und Endpunkte.	26. November 2023

Amazon GuardDuty hat die serviceverknüpfte Rolle (SLR) aktualisiert	GuardDuty hat neue Berechtigungen hinzugefügt, um Amazon ECS-Aktionen zum Verwalten und Abrufen von Informationen über die Amazon ECS-Cluster zu verwenden und die Amazon ECS-Kontoeinstellungen mit zu verwalten`guardduty Activate` . Die Aktionen im Zusammenhang mit Amazon ECS rufen auch die Informationen über die zugehörigen Tags ab. GuardDuty • Die folgenden Berechtigungen wurden im Rahmen der GuardDuty Erweiterung der Runtime Monitoring-Funktionen hinzugefügt: `"ecs:ListClusters", "ecs:DescribeClusters", "ecs:PutAccountSettingDefault"`	26. November 2023
Die AWS verwalteten Richtlinien wurden aktualisiert	GuardDuty hat dem AmazonGuardDutyFullAccessPolicyund eine neue Berechtigung hinzugefügt AmazonGuardDutyReadOnlyAccess. `organizations:ListAccounts`	16. November 2023

GuardDuty hat neue Befundtypen veröffentlicht, die EKS Audit Log Monitoring verwenden.	EKS Audit Log Monitoring unterstützt jetzt die folgenden Befundtypen im asiatisch-pazifischen Raum (Melbourne) (`ap-southeast-4`). • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	11. November 2023

GuardDuty veröffentlichte neue Befundtypen, die EKS Audit Log Monitoring verwenden.	EKS Audit Log Monitoring unterstützt jetzt die folgenden Befundtypen in den Regionen Asien-Pazifik (Hyderaba `dap-south-2`) (), Europa (Zürich`eu-central-2`) () und Europa (Spanien) (`eu-south-2`). • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	10. November 2023

- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

GuardDuty hat neue Befundtypen veröffentlicht, die EKS Audit Log Monitoring verwenden.	EKS Audit Log Monitoring unterstützt jetzt die folgenden Befundtypen. Diese Ergebnisarten sind in den Regionen Asien-Pazifik (Hyderabad) (`ap-south-2`), Europa (Zürich) (`eu-central-2`), Europa (Spanien) (`eu-south-2`) und Asien-Pazifik (Melbourne) (`ap-southeast-4`) noch nicht verfügbar. • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	8. November 2023

	• PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	
EKS-Laufzeit-Überwachung hat den neuen Agenten v1.3.1 veröffentlicht	EKS Runtime Monitoring hat eine neue Agentenversion 1.3.1 veröffentlicht, die wichtige Sicherheitspatches und Updates enthält.	23. Oktober 2023
Neues Filterattribut für die Erkenntnis	GuardDuty hat ein neues Kriterium hinzugefügt, um die generierten Ergebnisse zu filtern. Das Domänensuffix für DNS-Anfragen gibt die Domäne der zweiten und obersten Ebene an, die an der Aktivität beteiligt waren, die GuardDuty zur Generierung des Ergebnisses geführt hat.	17. Oktober 2023
EKS-Laufzeit-Überwachung hat den neuen Agenten v1.3.0 veröffentlicht, der Kubernetes Version 1.28 unterstützt	EKS Runtime Monitoring hat eine neue Agentenversion 1.3.0 veröffentlicht, die Kubernetes Version 1.28 unterstützt. Unterstützung für Ubuntu hinzugefügt. Weitere Informationen finden Sie in der Versionshistorie des EKS-Add-On-Agenten.	05. Oktober 2023

Für die Regionen Asien-Pazifik (Jakarta) und Naher Osten (VAE) wurden S3 und auf AWS CloudTrail maschinelem Lernen (ML) basierende Befundtypen hinzugefügt	In den Regionen Asien-Pazifik (Jakarta) und Naher Osten (GuardDutyVAE) sind jetzt die folgenden S3 und CloudTrail Ergebnisse zur Identifizierung des anomalen Verhaltens mithilfe des ML-Modells (Anomalieerkennung) verfügbar: • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior • Persistence:IAMUser/AnomalousBehavior • PrivilegeEscalation:IAMUser/AnomalousBehavior	20. September 2023

	• Discovery:IAMUser/AnomalousBehavior	
GuardDuty EKS Runtime Monitoring führt die Verwaltung des GuardDuty Security Agents auf Clusterebene ein	EKS Runtime Monitoring bietet Unterstützung für die Verwaltung des GuardDuty Security Agents für einzelne EKS-Cluster, um die Runtime-Ereignisse nur von diesen ausgewählten Clustern aus zu überwachen. EKS-Laufzeit-Überwachung erweitert diese Funktion um die Unterstützung von Tags.	13. September 2023
GuardDuty Malware Protection erweitert die Unterstützung auf mehr AWS-Regionen	Malware Protection ist jetzt in den Regionen Asien-Pazifik (Hyderabad), Asien-Pazifik (Melbourne), Europa (Zürich) und Europa (Spanien) verfügbar.	11. September 2023

GuardDuty ist jetzt in der Region Israel (Tel Aviv) verfügbar	Die Region Israel (Tel Aviv) wurde der Liste der Orte hinzugefügt AWS-Regionen , in denen sie jetzt verfügbar GuardDuty ist. Die folgenden Schutzpläne sind auch in der Region Israel (Tel Aviv) verfügbar: • GuardDuty EKS-Schutz umfasst EKS Audit Log Monitoring EKS-Laufzeit-Überwachung. • GuardDuty Lambda-Schutz. • GuardDuty Schutz vor Schadsoftware. • GuardDuty S3-Schutz. Weitere Informationen zur Verfügbarkeit von Schutzplä nen in der Region Israel (Tel Aviv) finden Sie unter Regionen und Endpunkte.	24. August 2023
GuardDuty Konfiguration zur automatischen Aktivieru ng für Ihre Organisation auf Schutzplanebene hinzugefügt	Aktualisieren Sie die Organisat ionskonfiguration für die Schutzpläne in Ihrer Region. Mögliche Konfigurationsopti onen sind entweder „für alle Konten aktivieren“, „für neue Konten automatisch aktiviere n“ oder „für kein Konto in Ihrer Organisation automatisch aktivieren“.	16. August 2023

S3-Erkennungstypen, die anomales Verhalten mithilfe GuardDuty des ML-Modells (Machine Learning) zur Erkennung von Anomalien identifizieren, sind jetzt im asiatisch-pazifischen Raum (Osaka) verfügbar	Die folgenden Erkenntnistypen sind jetzt in der Region Asien-Pazifik (Osaka) verfügbar: • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	10. August 2023
EKS-Laufzeit-Überwachung ist jetzt in Asien-Pazifik (Melbourne) verfügbar	Die EKS-Runtime-Überwachung innerhalb von GuardDuty EKS Protection bietet Runtime-Bedrohungserkennung für Ihre Amazon EKS-Cluster in der AWS Umgebung. Die Funktion wird jetzt in der Region Asien-Pazifik (Melbourne) unterstützt.	08. August 2023
Die Liste der GuardDuty Ergebnisse, die einen GuardDuty -initiierten Malware-Scan auslösen, wurde aktualisiert	Bestimmte Erkennungstypen von EKS Runtime Monitoring können jetzt einen GuardDuty -initiierten Malware-Scan in Ihrem aufrufen. AWS-Konto	19. Juli 2023

GuardDuty unterstützt 10.000 Mitgliedskonten durch AWS Organizations	Mit einem GuardDuty Administratorkonto können jetzt maximal 10.000 Mitgliedskonten verwaltet AWS Organizations werden. Dazu gehören auch maximal 5000 Mitgliedskonten, die auf Einladung mit dem GuardDuty Administratorkonto verknüpft wurden.	29. Juni 2023
EKS-Laufzeit-Überwachung kündigt drei neue Erkenntnistypen an.	EKS-Laufzeit-Überwachung unterstützt drei neue Erkenntnistypen, die auf der Prozessinjektions-Methode basieren. Die neuen Suchtypen lauten: Runtime/ DefenseEvasion .Proc, :Runtime/ .Ptrace und:Runtime/. ProcessInjection DefenseEvasion ProcessInjection DefenseEvasion ProcessInjection VirtualMemoryWrite.	22. Juni 2023
EKS-Laufzeit-Überwachung hat den neuen Agenten v1.2.0 veröffentlicht, der Kubernetes Version 1.27 unterstützt	EKS Runtime Monitoring hat eine neue Agentenversion 1.2.0 veröffentlicht, die auch ARM64-basierte Instanzen unterstützt. Unterstützung für Bottlerocket hinzugefügt. Weitere Informationen finden Sie in der Versionshistorie des EKS-Add-On-Agenten.	16. Juni 2023

GuardDuty Die Konsole bietet eine zusammengefasste Ansicht Ihrer Ergebnisse.	Das Übersichts-Dashboard in der GuardDuty Konsole bietet eine aggregierte Ansicht der GuardDuty Ergebnisse. Derzeit zeigt das Dashboard über verschiedene Widgets Daten für die letzten 10.000 Ergebnisse an, die für Ihr Konto (oder Mitgliedskonten, wenn Sie ein GuardDuty Administratorkonto haben) für die aktuelle Region generiert wurden.	12. Juni 2023
EKS Audit Log Monitoring ist jetzt in Asien-Pazifik (Hyderabad), Asien-Pazifik (Melbourne), Europa (Zürich) und Europa (Spanien) verfügbar	Aktivieren Sie EKS Audit Log Monitoring (in EKS Protection) für Ihre Konten, um EKS-Audit protokolle aus Ihren Amazon EKS-Clustern zu überwachen und sie auf potenziell bösartige und verdächtige Aktivitäten zu analysieren.	01. Juni 2023
EKS Audit Log Monitoring ist jetzt in Naher Osten (VAE) verfügbar	EKS Audit Log Monitoring ist jetzt im Nahen Osten (VAE) verfügbar. Aktivieren Sie EKS Audit Log Monitoring für Ihre Konten, um EKS-Audit protokolle aus Ihren Amazon EKS-Clustern zu überwachen und sie auf potenziell bösartige und verdächtige Aktivitäten zu analysieren.	3. Mai 2023

GuardDuty Malware Protection kündigt Malware-Scan auf Abruf an	Malware Protection hilft Ihnen dabei, das potenzielle Vorhandensein von Malware in den Amazon-EBS-Volumes zu erkennen, die Ihren Amazon-EC2-Instances und Container-Workloads angefügt sind. Es bietet jetzt zwei Arten von Scans: GuardDuty initiierte Scans und Scans auf Abruf. GuardDuty-initiierter Malware-Scan initiiert nur dann automatisch einen agentenlosen Scan in den Amazon EBS-Volumes, wenn eines der Ergebnisse GuardDuty generiert wird, die den -initiierten Malware-Scan auslösen. GuardDuty Sie können einen Malware-Scan auf Abruf für Amazon-EC2-Instances einleiten, indem Sie den Amazon-Ressourcennamen (ARN) angeben, der mit Ihrer Amazon-EC2-Instance verknüpft ist. Weitere Informationen darüber, wie sich die beiden Scantypen unterscheiden, finden Sie unter Malware Protection. • GuardDuty-initiierter Malware-Scan • Malware-Scan auf Abruf	27. April 2023

GuardDuty kündigt Lambda Protection an	Lambda Protection hilft Ihnen, potenzielle Sicherheitsbedrohungen in Ihren AWS Lambda -Funktionen zu erkennen. • Lambda-Protection-Erkenntnistypen • Behebung einer potenziell kompromittierten Lambda-Funktion	20. April 2023
GuardDuty ist jetzt in der Region Asien-Pazifik (Melbourne) verfügbar	Asien-Pazifik (Melbourne) wurde der Liste der verfügbaren AWS-Regionen GuardDuty Orte hinzugefügt. Informationen darüber, welche Funktionen in dieser Region verfügbar sind, finden Sie unter Regionen und Endpunkte.	19. April 2023

GuardDuty 3 neue EC2-Befundtypen hinzugefügt	GuardDuty führt neue Erkennungstypen ein, um die Verwendung externer DNS-Resolver und verschlüsselter DNS-Technologien zu erkennen. Informationen darüber AWS-Regionen , wo diese Suchtypen unterstützt werden, finden Sie unter Regionen und Endpunkte. • DefenseEvasion:EC2/UnusualDNSResolver • DefenseEvasion:EC2/UnusualDoHActivity • DefenseEvasion:EC2/UnusualDoTActivity	5. April 2023

GuardDuty kündigt EKS Runtime Monitoring in EKS Protection an	Die EKS-Runtime-Überwachung innerhalb von EKS Protection bietet Runtime-Bedrohungserkennung für Ihre Amazon EKS-Cluster in der AWS Umgebung. Die Funktion verwendet einen Amazon-EKS-Add-On-Agenten (`aws-guardduty-agent`), der Laufzeit-Ereignisse aus Ihren EKS-Workloads sammelt. Nach dem GuardDuty Empfang dieser Runtime-Ereignisse werden sie überwacht und analysiert, um potenzielle verdächtige Sicherheitsbedrohungen zu identifizieren. Weitere Informationen finden Sie unter Erkenntnisdetails und Erkenntnistypen der EKS-Laufzeit-Überwachung.	30. März 2023

GuardDuty fügt eine neue Funktionalität hinzu — `autoEnableOrganizationMembers`	Amazon GuardDuty fügt eine neue Organisationskonfigurationsoption hinzu, mit der GuardDuty Administratorkonten geprüft und (falls erforderlich) durchgesetzt werden können. Diese Option GuardDuty ist für `ALL` die Mitglieder ihrer Organisation aktiviert. Die beste Vorgehensweise besteht jetzt darin, `autoEnableOrganizationMembers` anstelle von `autoEnable` zu verwenden. `autoEnable` ist veraltet, wird aber immer noch unterstützt. Die folgenden APIs sind von dieser neuen Funktionalität betroffen: • DescribeOrganizationConfiguration • UpdateOrganizationConfiguration • DisassociateMembers • DeleteMembers • DisassociateFromAdministratorAccount • StopMonitoringMembers	23. März 2023

Die RDS-Schutzfunktion in Amazon GuardDuty ist jetzt allgemein verfügbar	GuardDuty RDS Protection überwacht und profiliert die RDS-Anmeldeaktivitäten, um verdächtiges Anmeldeverhalten auf Ihren Amazon Aurora Aurora-Datenbank-Instances zu identifizieren. Weitere Informationen dazu, welche AWS-Regionen unterstützen, finden Sie unter Regionen und Endpunkte.	16. März 2023

GuardDuty kündigt die Aktivierung der Funktion an	In der Vergangenheit ermöglichte die GuardDuty API die Konfiguration sowohl von Funktionen als auch von Datenquellen, aber jetzt werden alle neuen GuardDuty Schutztypen als Funktione n und nicht als Datenquel len konfiguriert. GuardDuty unterstützt weiterhin die Datenquellen über die API, fügt aber keine neue API hinzu. Die Aktivierung von Funktionen wirkt sich auf das Verhalten der APIs aus, die zur Aktivierung verwendet werden, GuardDuty oder auf einen darin enthaltenen Schutztyp GuardDuty. Wenn Sie Ihre GuardDuty Konten über eine API, ein SDK oder eine CFN-Vorlage verwalten , finden Sie weitere Informati onen unter GuardDuty API-Änderungen im März 2023.	16. März 2023
GuardDuty Der Malware-S chutz ist jetzt in der Region Naher Osten (VAE) verfügbar	Die Malware-Schutzfunktion in GuardDuty wird in der Region Naher Osten (VAE) unterstüt zt. Weitere Informationen finden Sie unter Regionen und Endpunkte.	13. März 2023

Amazon GuardDuty hat die serviceverknüpfte Rolle (SLR) aktualisiert	GuardDuty hat die folgenden neuen Berechtigungen hinzugefügt, um die kommende Funktion GuardDuty EKS Runtime Monitoring zu unterstützen. • Verwenden Sie Amazon-EKS-Aktionen, um Informationen über die EKS-Cluster zu verwalten und abzurufen und EKS-Add-Ons auf EKS-Clustern zu verwalten. Die EKS-Aktionen rufen auch die Informationen über die zugehörigen Tags ab GuardDuty. `"eks:ListClusters", "eks:DescribeCluster", "ec2:DescribeVpcEndpointServices", "ec2:DescribeSecurityGroups"`	08. März 2023
Amazon GuardDuty hat die serviceverknüpfte Rolle (SLR) aktualisiert	Die GuardDuty Spiegelreflexkamera wurde aktualisiert und ermöglicht nun die Erstellung von Malware Protection SLR, nachdem der Malware-Schutz aktiviert wurde.	21. Februar 2023

GuardDuty erfordert TLS v1.2 oder höher	Für die Kommunikation mit AWS Ressourcen wird TLS v1.2 oder höher GuardDuty benötigt und unterstützt. Weitere Informationen finden Sie unter Datenschutz und Infrastruktursicherheit.	14. Februar 2023
GuardDuty ist jetzt in der Region Asien-Pazifik (Hyderabad) verfügbar	Die Region Asien-Pazifik (Hyderabad) wurde zur Liste der verfügbaren AWS-Regionen Regionen hinzugefügt. GuardDuty Weitere Informationen finden Sie unter Regionen und Endpunkte.	14. Februar 2023
Das GuardDuty Amazon-Benutzerhandbuch entspricht den Best Practices für IAM	Aktualisierter Leitfaden, angepasst an die bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte IAM-Methoden.	10. Februar 2023
GuardDuty ist jetzt in der Region Europa (Spanien) verfügbar	Europa (Spanien) wurde zur Liste der AWS-Regionen verfügbaren GuardDuty Standorte hinzugefügt. Weitere Informationen finden Sie unter Regionen und Endpunkte.	8. Februar 2023
GuardDuty ist jetzt in der Region Europa (Zürich) verfügbar	Europa (Zürich) wurde zur Liste der AWS-Regionen verfügbaren GuardDuty Standorte hinzugefügt. Weitere Informationen finden Sie unter Regionen und Endpunkte.	12. Dezember 2022

Vorabversion einer neuen Funktion — GuardDuty RDS Protection	GuardDuty RDS Protection überwacht und profiliert die RDS-Anmeldeaktivitäten, um verdächtiges Anmeldeverhalten auf Ihren Amazon Aurora Aurora-Datenbank-Instances zu identifizieren. Derzeit ist es als Vorabversion in fünf AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Regionen und Endpunkte.	30. November 2022
GuardDuty ist jetzt in der Region Naher Osten (VAE) verfügbar	Naher Osten (VAE) zur Liste der AWS-Regionen verfügbaren GuardDuty Produkte hinzugefügt. Weitere Informationen finden Sie unter Regionen und Endpunkte.	6. Oktober 2022

Inhalt für eine neue Funktion hinzugefügt — GuardDuty Malware-Schutz	GuardDuty Malware Protection ist eine optionale Erweiterung für Amazon GuardDuty. Malware Protection GuardDuty identifiziert zwar die gefährdeten Ressourcen, erkennt aber auch die Malware, die die Quelle der Bedrohung sein könnte. Wenn der Malware-Schutz aktiviert ist, initiiert Malware Protection jedes Mal, wenn verdächtiges Verhalten auf einer Amazon EC2 EC2-Instance oder einem Container-Workload GuardDuty entdeckt wird, der auf Malware hinweist, einen agentenlosen Scan auf den EBS-Volumes, die an die betroffenen EC2-Instance- oder Container-Workloads angehängt sind, um das Vorhandensein von GuardDuty Malware zu erkennen. Informationen zur Funktionsweise von Malware Protection und zur Konfiguration dieser Funktion finden Sie unter Malware-Schutz. GuardDuty • Informationen zu den Erkenntnissen von Malware Protection finden Sie unter Erkenntnis-Details. • Informationen zur Behebung der gefährdeten EC2-Insta	26. Juli 2022

	nce und eines eigenstän digen Containers finden Sie unter Behebung von Sicherheitsproblemen, die von entdeckt wurden. GuardDuty • Informationen zur Überwachung von CloudWatch Protokollen für Malware-Scans und zu den Gründen für das Übersprin gen einer Ressource beim Malware-Scan finden Sie unter Grundlegendes CloudWatch zu Protokoll en und Gründen für das Überspringen von Dateien. • Informationen zu falsch positiven Bedrohung serkennungen finden Sie unter Falschmeldungen im GuardDuty Malware-Schutz melden.	
Ein Erkenntnistyp wurde außer Betrieb genommen	Exfiltration:S3/ObjectRead. Unusual wurde außer Betrieb genommen.	5. Juli 2022

Es wurden neue S3-Findetypen hinzugefügt, die anomales Verhalten mithilfe GuardDuty des ML-Modells (Machine Learning) zur Erkennung von Anomalien identifizieren.	Die folgenden neuen S3-Erkenntnistypen wurden hinzugefügt. Diese Erkenntnistypen identifizieren, ob eine API-Anfrage eine IAM-Entität auf ungewöhnliche Weise aufgerufen hat. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Taktiken von Angreifern in Verbindung gebracht werden. Weitere Informationen zu den einzelnen neuen Erkenntnissen finden Sie unter S3-Erkenntnistypen. • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	5. Juli 2022

Es wurden GuardDuty EKS-Schutzinhalte hinzugefügt für GuardDuty	GuardDuty kann jetzt durch die Überwachung von EKS-Auditprotokollen Ergebnisse für Ihre Amazon EKS-Ressourcen generieren. Informationen zur Konfiguration dieser Funktion finden Sie unter EKS-Schutz in Amazon GuardDuty. Eine Liste der Ergebnisse, die für Amazon EKS-Ressourcen generiert werden GuardDuty können, finden Sie unter Ergebnisse von Kubernetes. Es wurden neue Anleitungen zur Behebung hinzugefügt, um die Behebung dieser Erkenntnisse zu unterstützen im Leitfaden zur Behebung von Erkenntnissen in Kubernetes.	25 Januar 2022
Es wurde eine neue Erkenntnis hinzugefügt	Die neue Erkenntnis UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS wurde hinzugefügt. Dieses Ergebnis informiert Sie darüber, wenn ein AWS Konto außerhalb Ihrer Umgebung auf Ihre Instance-Anmeldeinformationen zugreift. AWS	20. Januar 2022

Die Erkenntnistypen wurden aktualisiert, um Probleme im Zusammenhang mit log4j leichter identifizieren zu können	Amazon GuardDuty hat die folgenden Suchtypen aktualisiert, um Probleme im Zusammenhang mit CVE-2021-44228 und CVE-2021-45046 zu identifiz ieren und zu priorisieren: Backdoor:EC2/C&CActivity.B; Backdoor:EC2/C&CAcactivity. B! DNSNetworkPortUnusual; Verhalten: EC2/.	22. Dezember 2021
Erkenntnis-Änderungen	UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltrat ion wurde geändert zu UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltrat ion.OutsideAWS. Diese verbesserte Version der Erkenntnisse erfasst die typischen Standorte, von denen aus Ihre Anmeldein formationen verwendet werden, und reduziert so die Anzahl der Erkenntnisse aus dem Datenverkehr, der über lokale Netzwerke geleitet wird. UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltrat ion.OutsideAWS	7. September 2021
GuardDuty Update auf SLR	Die GuardDuty Spiegelre flexkamera wurde mit neuen Maßnahmen zur Verbesser ung der Suchgenauigkeit aktualisiert.	3. August 2021

Es wurden Datenquelleninformationen für jeden Erkenntnistyp hinzugefügt.	Die Beschreibungen der Ergebnisse enthalten jetzt Informationen über Datenquellen, die zur Generierung dieses Ergebnisses GuardDuty verwendet wurden.	10. Mai 2021
13 Erkenntnistypen entfernt.	13 Ergebnisse wurden zurückgezogen, um durch neue AnomalousBehavoir Ergebnisse ersetzt zu werden. Persistence:IAMUser/NetworkPermissions, Persistence:IAMUser/ResourcePermissions, Persistence:IAMUser/UserPermissions, PrivilegeEscalation:IAMUser/AdministrativePermissions, Recon:IAMUser/NetworkPermissions, Recon:IAMUser/ResourcePermissionsRecon:IAMUser/UserPermissions, ResourceConsumption:IAMUser/ComputeResources, Stealth:IAMUser/LoggingConfigurationModified, Discovery:S3/BucketEnumeration.Unusual, Impact:S3/ObjectDelete.Unusual, Impact:S3/PermissionsModification.Unusual.	12. März 2021

Es wurden 8 neue Erkenntnistypen für anomales Verhalten hinzugefügt.	Es wurden 8 neue IAMUser-Erkenntnistypen hinzugefügt, die auf anomalem Verhalten für IAM-Prinzipale basieren. CredentialAccess:IAMUser/AnomalousBehavior, DefenseEvasion:IAMUser/AnomalousBehavior, Discovery:IAMUser/AnomalousBehavior, Exfiltration:IAMUser/AnomalousBehavior, Impact:IAMUser/AnomalousBehavior, InitialAccess:IAMUser/AnomalousBehavior, Persistence:IAMUser/AnomalousBehavior, PrivilegeEscalation:IAMUser/AnomalousBehavior.	12. März 2021
EC2-Erkenntnisse basierend auf der Domain-Reputation wurden hinzugefügt.	Es wurden 4 neue Arten von Erkenntnistypen hinzugefügt, die auf der Domain-Reputation basieren. Impact:EC2/AbusedDomainRequest.Reputation , Impact:EC2/BitcoinDomainRequest.Reputation, Impact:EC2/MaliciousDomainRequest.Reputation. Außerdem wurde eine neue EC2-Erkenntnis für C&CActivity hinzugefügt. Impact:EC2/SuspiciousDomainRequest.Reputation	27. Januar 2021

Es wurden 4 neue Erkenntnistypen hinzugefügt.	Es wurden 3 neue S3-MaliciousIPCaller-Erkenntnisse hinzugefügt. Discovery:S3/MaliciousIPCaller, Exfiltration:S3/MaliciousIPCaller, Impact:S3/MaliciousIPCaller. Außerdem wurde eine neue EC2-Erkenntnis für C&CActivity hinzugefügt. Backdoor:EC2/C&CActivity.B	21. Dezember 2020
Der Erkenntnistyp UnauthorizedAccess:EC2/TorIPCaller wurde außer Betrieb genommen.	Der UnauthorizedAccess:EC2/TorIPCaller Befundtyp ist jetzt nicht mehr gültig GuardDuty. Weitere Informationen.	1. Oktober 2020
Der Erkenntnistyp Impact:EC2/WinRmBruteForce wurde hinzugefügt.	Eine neue Auswirkungs-Erkenntnis Impact:EC2/WinRmBruteForce wurde hinzugefügt. Weitere Informationen.	17. September 2020
Der Erkenntnistyp Impact:EC2/PortSweep wurde hinzugefügt.	Eine neue Auswirkungs-Erkenntnis Impact:EC2/PortSweep wurde hinzugefügt. Weitere Informationen.	17. September 2020
GuardDuty ist jetzt in den Regionen Afrika (Kapstadt) und Europa (Mailand) verfügbar.	Afrika (Kapstadt) und Europa (Mailand) wurden zur Liste der AWS Regionen hinzugefügt, in denen diese Option verfügbar GuardDuty ist. Weitere Informationen	31. Juli 2020

Es wurden neue Nutzungsdetails für die GuardDuty Kostenüberwachung hinzugefügt.	Sie können jetzt neue Messwerte verwenden, um GuardDuty Nutzungskostendaten für Ihr Konto und die von Ihnen verwalteten Konten abzufragen. Eine neue Übersicht der Nutzungskosten ist in der Konsole unter https://console.aws.amazon.com/guardduty/ verfügbar. Detailliertere Informationen können über die API abgerufen werden.	31. Juli 2020
Es wurden Inhalte zum S3-Schutz durch die Überwachung von S3-Datenereignissen in hinzugefügt GuardDuty.	GuardDuty S3 Protection ist jetzt durch die Überwachung von Ereignissen auf der S3-Datenebene als neue Datenquelle verfügbar. Bei neuen Konten wird dieses Feature automatisch aktiviert. Wenn Sie die neue Datenquelle bereits verwenden, können GuardDuty Sie sie für sich selbst oder Ihre Mitgliedskonten aktivieren.	31. Juli 2020
Es wurden 14 neue S3-Erkenntnisse hinzugefügt.	14 neue S3-Erkenntnistypen wurden für Quellen der S3-Steuerebene und -Datenebene hinzugefügt.	31. Juli 2020

Zusätzliche Unterstützung für S3-Erkenntnisse hinzugefügt und zwei vorhandene Erkenntnistyp-Namen geändert.	GuardDuty Die Ergebnisse enthalten jetzt mehr Details zu Ergebnissen, die S3-Buckets betreffen. Bestehende Erkenntnistypen, die sich auf die S3-Aktivität bezogen, wurden umbenannt: Policy:IAMUser/S3BlockPublicAccessDisabled wurde zu Policy:S3/BucketBlockPublicAccessDisabled geändert. Stealth:IAMUser/S3ServerAccessLoggingDisabled wurde geändert zu Stealth:S3/ServerAccessLoggingDisabled.	28. Mai 2020

Inhalt für die AWS Organizations Integration hinzugefügt.	GuardDuty lässt sich jetzt mit AWS Organizations delegierten Administratoren integrieren, sodass Sie GuardDuty Konten innerhalb Ihrer Organisation verwalten können. Wenn Sie einen delegierten Administrator als Ihr GuardDuty Administratorkonto festlegen, können Sie automatisch GuardDuty für jedes Organisationsmitglied die Verwaltung durch das delegierte Administratorkonto aktivieren. Sie können die automatische Aktivierung auch GuardDuty bei neuen AWS Organizations Mitgliedskonten vornehmen. Weitere Informationen.	20. April 2020
Inhalt für das Feature zum Export von Erkenntnissen hinzugefügt.	Inhalt hinzugefügt, der die Funktion „Ergebnisse exportieren“ von beschreibt GuardDuty.	14. November 2019
Der Erkenntnistyp UnauthorizedAccess:EC2/MetadataDNSRebind wurde hinzugefügt.	Eine neue unautorisierte Erkenntnis UnauthorizedAccess:EC2/MetadataDNSRebind wurde hinzugefügt. Weitere Informationen.	10. Oktober 2019
Der Erkenntnistyp Stealth:IAMUser/S3ServerAccessLoggingDisabled wurde hinzugefügt.	Eine neue Stealth-Erkenntnis Stealth:IAMUser/S3ServerAccessLoggingDisabled wurde hinzugefügt. Weitere Informationen.	10. Oktober 2019

Der Erkenntnistyp Policy:IAMUser/S3BlockPublicAccessDisabled wurde hinzugefügt.	Eine neue Richtlinien-Erkenntnis Policy:IAMUser/S3BlockPublicAccessDisabled wurde hinzugefügt. Weitere Informationen.	10. Oktober 2019
Der Erkenntnistyp Backdoor:EC2/XORDDOS wurde außer Betrieb genommen.	Der Backdoor:EC2/XORDDOS Befundtyp ist jetzt nicht mehr verfügbar GuardDuty. Erfahren Sie mehr	12. Juni 2019
Der Erkenntnistyp Privilege Escalation wurde hinzugefügt.	Der PrivilegeEscalation-Erkenntnistyp erkennt, wenn Benutzer versuchen, ihren Konten eskalierte Berechtigungen mit weniger Einschränkungen zuzuweisen. Weitere Informationen	14. Mai 2019
GuardDuty ist jetzt in der Region Europa (Stockholm) verfügbar.	Europa (Stockholm) wurde zur Liste der AWS Regionen hinzugefügt, in denen GuardDuty es verfügbar ist. Weitere Informationen	9. Mai 2019
Ein neuer Erkenntnistyp Recon:EC2/PortProbeEMRUnprotectedPort wurde hinzugefügt.	Dieses Ergebnis informiert Sie darüber, dass ein EMR-bezogener sensibler Port auf einer EC2-Instance nicht gesperrt ist und aktiv geprüft wird. Weitere Informationen	8. Mai 2019

Es wurden 5 neue Erkenntnistypen hinzugefügt, die erkennen, wenn Ihre EC2-Instances für Denial-of-Service (DoS)-Angriffe genutzt werden.	Diese Ergebnisse informieren Sie von EC2-Instances in Ihrer Umgebung, deren Verhalten darauf hinweist, dass sie möglicherweise für Denial-of-Service (DoS)-Angriffe genutzt werden. Weitere Informationen	8. März 2019
Ein neuer Erkenntnistyp Policy:IAMUser/RootCredentialUsage wurde hinzugefügt.	Policy:IAMUser/RootCredentialUsageDer Suchtyp informiert Sie darüber, dass Ihre Root-Benutzeranmeldedaten verwendet AWS-Konto werden, um programmatische Anfragen an Dienste zu AWS stellen. Weitere Informationen	24. Januar 2019
Der UnauthorizedAccess:IAMUser/UnusualASNCaller-Erkenntnistyp wurde außer Betrieb genommen	Der UnauthorizedAccess:IAMUser/UnusualASNCaller-Erkenntnistyp wurde außer Betrieb genommen. Sie werden nun über Aktivitäten informiert, die von ungewöhnlichen Netzwerken aus über andere aktive GuardDuty Suchtypen aufgerufen wurden. Der generierte Ergebnistyp basiert auf der Kategorie der API, die von einem unüblichen Netzwerk aufgerufen wurde. Weitere Informationen	21. Dezember 2018

Zwei neue Erkenntnistypen wurden hinzugefügt: PenTest:IAMUser/ParrotLinux und PenTest:IAMUser/PentooLinux	Der PenTest:IAMUser/ParrotLinux-Erkenntnistyp informiert Sie darüber, dass ein Computer, auf dem Parrot Security Linux ausgeführt wird, API-Aufrufe mit Anmeldeinformationen durchführt, die zu Ihrem AWS -Konto gehören. Der PenTest:IAMUser/PentooLinux-Erkenntnistyp informiert Sie darüber, dass ein Computer, auf dem Pentoo Linux ausgeführt wird, API-Aufrufe mit Anmeldeinformationen durchführt, die zu Ihrem AWS -Konto gehören. Weitere Informationen	21. Dezember 2018
Unterstützung für das SNS-Thema GuardDuty Amazon-Ankündigungen hinzugefügt	Sie können jetzt das SNS-Thema GuardDuty Ankündigungen abonnieren, um Benachrichtigungen über neu veröffentlichte Ergebnisarten, Aktualisierungen der vorhandenen Befundtypen und andere Funktionsänderungen zu erhalten. Benachrichtigungen sind in allen Formaten verfügbar, die Amazon SNS unterstützt. Weitere Informationen	21. November 2018

Zwei neue Erkenntnistypen wurden hinzugefügt: UnauthorizedAccess:EC2/TorClient und UnauthorizedAccess:EC2/TorRelay	UnauthorizedAccess:EC2/TorClientFinding Type informiert dich darüber, dass eine EC2-Instance in deiner AWS Umgebung Verbindungen zu einem Tor Guard- oder einem Authority-Knoten herstellt. UnauthorizedAccess:EC2/TorRelayDie Suche nach dem Typ informiert dich darüber, dass eine EC2-Instance in deiner AWS Umgebung Verbindungen zu einem Tor-Netzwerk auf eine Weise herstellt, die darauf hindeutet, dass sie als Tor-Relay fungiert. Weitere Informationen	16. November 2018
Ein neuer Erkenntnistyp CryptoCurrency:EC2/BitcoinTool.B wurde hinzugefügt.	Dieses Ergebnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS Umgebung einen Domainnamen abfragt, der mit Bitcoin oder einer anderen kryptowährungsbezogenen Aktivität verknüpft ist. Weitere Informationen	9. November 2018

Unterstützung für die Aktualisierung der Häufigkeit von Benachrichtigungen, die an Ereignisse gesendet werden, hinzugefügt CloudWatch	Sie können jetzt die Häufigkeit der an CloudWatch Ereignisse gesendeten Benachrichtigungen für das spätere Auftreten vorhandener Ergebnisse aktualisieren. Mögliche Werte sind 15 Minuten, 1 Stunde oder standardmäßig 6 Stunden. Weitere Informationen	9. Oktober 2018
Zusätzliche Unterstützung für Regionen hinzugefügt	Unterstützung für Regionen AWS GovCloud (US-West) hinzugefügt Erfahren Sie mehr	25. Juli 2018
Unterstützung für AWS CloudFormation StackSets in hinzugefügt GuardDuty	Sie können die GuardDuty Vorlage „Amazon aktivieren“ verwenden, um die Aktivierung GuardDuty gleichzeitig in mehreren Konten durchzuführen. Weitere Informationen	25. Juni 2018

Unterstützung für Regeln zur GuardDuty automatischen Archivierung hinzugefügt	Kunden können jetzt granulare Regeln für die automatische Archivierung erstellen, um Ergebnisse zu unterdrücken. Markiert Ergebnisse, die einer Regel für die automatische Archivierung entsprechen, GuardDuty automatisch als archiviert. Auf diese Weise können Kunden weitere Anpassungen GuardDuty vornehmen, sodass nur relevante Ergebnisse in der Tabelle mit den aktuellen Ergebnissen angezeigt werden. Weitere Informationen	4. Mai 2018
GuardDuty ist in der Region Europa (Paris) verfügbar	GuardDuty ist jetzt in Europa (Paris) verfügbar, sodass Sie die kontinuierliche Sicherheitsüberwachung und Bedrohungserkennung in dieser Region ausweiten können. Weitere Informationen	29. März 2018
Das Erstellen von GuardDuty Administratorkonten und Mitgliedskonten über AWS CloudFormation wird jetzt unterstützt.	Weitere Informationen finden Sie unter `AWS::GuardDuty::master` und `AWS::GuardDuty::member`.	6. März 2018
Neun neue CloudTrail basierte Anomalieerkennungen wurden hinzugefügt.	Diese neuen Erkennungstypen werden automatisch GuardDuty in allen unterstützten Regionen aktiviert. Weitere Informationen	28. Februar 2018

Es wurden drei neue Erkennungsmöglichkeiten von Bedrohungen (Erkenntnistypen) hinzugefügt.	Diese neuen Suchtypen werden automatisch GuardDuty in allen unterstützten Regionen aktiviert. Weitere Informationen	5. Februar 2018
Erhöhung des Limits für GuardDuty Mitgliedskonten.	Mit dieser Version können Sie bis zu 1000 GuardDuty Mitgliedskonten pro AWS Konto hinzufügen (GuardDuty Administratorkonto). Weitere Informationen	25. Januar 2018
Änderungen beim Upload und bei der weiteren Verwaltung von Listen vertrauenswürdiger IP-Adressen und Bedrohungslisten für GuardDuty Administratorkonten und Mitgliedskonten.	Mit dieser Version können Benutzer mit GuardDuty Administratorkonten vertrauenswürdige IP-Listen und Bedrohungslisten hochladen und verwalten. Benutzer mit GuardDuty Mitgliedskonten können keine Listen hochladen und verwalten. Vertrauenswürdige IP-Adressen und Bedrohungslisten, die vom Administratorkonto hochgeladen werden, wirken sich negativ auf die GuardDuty Funktionalität der Mitgliedskonten aus. Weitere Informationen	25. Januar 2018

Frühere Aktualisierungen

Änderung	Beschreibung	Datum
Erste Veröffentlichung	Erstveröffentlichung des GuardDuty Amazon-Benutzerhandbuchs.	28. November 2017

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.