AWS Security Incident Response Benutzerleitfaden

Version March 27, 2026

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Security Incident Response Benutzerleitfaden:

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Was ist AWS Security Incident Response?

AWS Security Incident Response hilft Ihnen, sich schnell auf Sicherheitsvorfälle vorzubereiten, darauf zu reagieren und Anleitungen zu erhalten, um sich nach Sicherheitsvorfällen zu erholen. Dazu gehören Vorfälle wie Kontoübernahmen, Datenschutzverletzungen und Ransomware-Angriffe.

AWS Security Incident Response analysiert die erkannten Bedrohungen, eskaliert Sicherheitsereignisse und managt Fälle, die Ihre sofortige Aufmerksamkeit erfordern. Darüber hinaus haben Sie Zugriff auf Security Incident Response-Techniker, die die betroffenen Ressourcen untersuchen.

> **Note**
>
> Es gibt keine Garantie dafür, dass die betroffenen Ressourcen wiederhergestellt werden können. Wir empfehlen, Backups für Ressourcen einzurichten und zu verwalten, die sich auf Ihre Geschäftsanforderungen auswirken könnten.

AWS Security Incident Response arbeitet mit anderen AWS Detection and Response Services zusammen und begleitet Sie durch den gesamten Incident-Lebenszyklus — von der Erkennung bis zur Wiederherstellung.

Inhalt

Unterstützte Konfigurationen

AWS Security Incident Response unterstützt die folgenden Sprach- und Regionskonfigurationen:

- Sprache: AWS Security Incident Response bietet speziellen englischen Support. Der Support in japanischer Sprache ist auf die Geschäftszeiten der Japan Standardzeit beschränkt und unterliegt bestimmten Einschränkungen:

- > **Note**
  >
  > Support in japanischer Sprache wird während der Geschäftszeiten (09:00 bis 17:00 Uhr, Montag bis Freitag, außer an Feiertagen) nach bestem Wissen und Gewissen bereitgestellt

- AWS Unterstützte Regionen:

  AWS Security Incident Response ist in einer Teilmenge von AWS-Regionen verfügbar. In diesen unterstützten Regionen können Sie eine Mitgliedschaft erstellen, Kundenvorgänge erstellen und anzeigen und auf das Dashboard zugreifen.

  - USA Ost (Ohio)
  - USA West (Oregon)
  - USA Ost (Virginia)
  - Europe (Frankfurt)
  - Europa (Irland)
  - Europa (London)
  - Europa (Milan)
  - Europa (Paris)
  - Europa (Spain)
  - Europa (Stockholm)
  - Europa (Zürich)
  - Asien-Pazifik (Hongkong)
  - Asien-Pazifik (Hyderabad)
  - Asien-Pazifik (Jakarta)
  - Asien-Pazifik (Melbourne)
  - Asien-Pazifik (Mumbai)
  - Asia Pacific (Seoul)
  - Asien-Pazifik (Singapur)
  - Asien-Pazifik (Sydney)
  - Asien-Pazifik (Tokio)
  - Canada (Central)
  - Middle East (Bahrain)
  - Naher Osten (VAE)

- Südamerika (São Paulo)
- Afrika (Kapstadt)

Wenn Sie die Überwachungs- und Ermittlungsfunktion aktivieren, werden GuardDuty Amazon-Ergebnisse aus allen aktiven Werbespots AWS Security Incident Response überwacht AWS-Regionen. Aus Sicherheitsgründen AWS empfiehlt es sich, die Aktivierung GuardDuty in allen unterstützten AWS Regionen zu aktivieren. Diese Konfiguration GuardDuty ermöglicht es, Erkenntnisse über nicht autorisierte oder ungewöhnliche Aktivitäten zu generieren, selbst AWS-Regionen wenn Sie Ressourcen nicht aktiv einsetzen. Auf diese Weise verbessern Sie Ihre allgemeine Sicherheitslage und sorgen für eine umfassende Bedrohungserkennung in Ihrer gesamten AWS Umgebung.

> **Note**
>
> Amazon GuardDuty meldet Ergebnisse für konfigurierte Regionen. Wenn Sie den Service in einer bestimmten Region nicht aktivieren möchten, sind keine Benachrichtigungen verfügbar.

Zusammenfassung der Funktionen

Überwachung und Untersuchung

AWS Security Incident Response überprüft schnell Sicherheitsbedrohungen von Amazon GuardDuty und Integrationen von Drittanbietern und reduziert so die Anzahl der Analysen AWS Security Hub CSPM, die Ihr Team analysieren muss. Es konfiguriert Unterdrückungsregeln auf der Grundlage Ihrer Umgebung, um die Anzahl der Bedrohungswarnungen zu reduzieren, die Sie analysieren und untersuchen müssen.

Optimieren Sie die Reaktion auf Vorfälle

Skalieren und implementieren Sie die Reaktion auf Vorfälle innerhalb von Minuten mit relevanten Stakeholdern, Diensten und Tools von Drittanbietern.

Self-Service-Sicherheitslösungen

AWS Security Incident Response bietet APIs die Möglichkeit, Ihre eigenen maßgeschneiderten Sicherheitslösungen zu integrieren und Ihnen die Möglichkeit zu geben, Ihre eigenen maßgeschneiderten Sicherheitslösungen zu entwickeln.

Dashboard für mehr Transparenz

Überwachen und messen Sie die Bereitschaft zur Reaktion auf Vorfälle.

Sicherheitslage

Greifen Sie auf AWS bewährte Verfahren und geprüfte Tools zur Sicherheitsbeurteilung und schnellen Untersuchung von Vorfällen zu.

Beschleunigte Unterstützung

Setzen Sie sich mit den Security Incident Response-Technikern in Verbindung, um Sicherheitsvorfälle zu untersuchen, einzudämmen und Ratschläge zu erhalten, wie Sie sich nach Sicherheitsereignissen erholen können.

Bereitschaft und Einsatzbereitschaft

Implementieren Sie optimierte Benachrichtigungen, indem Sie Ihr Incident Response-Team einrichten, das mithilfe vordefinierter Berechtigungsrichtlinien Benachrichtigungen an bestimmte Personen oder Gruppen ausgibt.

Konzepte und Terminologie

Die folgenden Begriffe und Konzepte sind wichtig, um den AWS Security Incident Response Service und seine Funktionsweise zu verstehen.

Umfang: AWS Security Incident Response Entspricht dem Leitfaden 800-61 des National Institute of Standards and Technology (NIST) zur Behandlung von Computersicherheitsvorfällen und bietet einen konsistenten Ansatz für das Management von Sicherheitsereignissen, der sich auf die bewährten Verfahren der Branche bezieht.

Analyse: Die detaillierte Untersuchung und Untersuchung eines Sicherheitsvorfalls, um seinen Umfang, seine Auswirkungen und seine Ursache zu verstehen.

AWS Security Incident Response Serviceportal: Ein Self-Service-Portal, über das Sie Fälle von Sicherheitsvorfällen einleiten und verwalten können. Die kontinuierliche Kommunikation und Berichterstattung wird durch das Ticketsystem, automatisierte Benachrichtigungen und die direkte Zusammenarbeit mit dem Serviceteam erleichtert.

Kommunikation: Der kontinuierliche Dialog und der Informationsaustausch zwischen dem AWS Security Incident Response Team und dem Kunden während des Incident-Response-Prozesses.

Eindämmung, Beseitigung und Wiederherstellung: Verhinderung zusätzlicher unberechtigter Aktivitäten (Eindämmung) in Verbindung mit der Entfernung nicht autorisierter Ressourcen und der ursprünglichen Sicherheitslücke (Beseitigung) sowie der Wiederherstellung von Ressourcen, um wieder normal arbeiten zu können.

Kontinuierliche Verbesserung: AWS Security Incident Response berücksichtigt Feedback und Erfahrungen aus früheren Projekten, um die Erkennungskapazitäten, Ermittlungsprozesse und Abhilfemaßnahmen zu verbessern. AWS Security Incident Response hält sich auch up-to-date über die neuesten Sicherheitsbedrohungen und bewährte Verfahren zur Bewältigung neuer Sicherheitsprobleme auf dem Laufenden.

Cybersicherheitsereignis: Eine Aktion, bei der ein Informationssystem oder ein Netzwerk genutzt wird, um negative Auswirkungen auf das System, das Netzwerk oder die darin enthaltenen Informationen zu haben.

Cybersicherheitsvorfall: Ein Verstoß oder die unmittelbare Gefahr eines Verstoßes gegen Computersicherheitsrichtlinien, Richtlinien zur zulässigen Nutzung oder Standardsicherheitspraktiken.

Techniker zur Reaktion auf Sicherheitsvorfälle: Eine Gruppe von Personen, die bei aktiven Sicherheitsereignissen Unterstützung leisten. Für AWS unterstützte Fälle sind dies die Security Incident Response Engineers.

Workflow zur Reaktion auf Vorfälle: Die festgelegte Abfolge von Schritten und Aktivitäten im Zusammenhang mit der end-to-end Verwaltung eines Sicherheitsereignisses gemäß dem Standard NIST 800-61.

Investigative Tools: AWS Security Incident Response Tools und dienstbezogene Rollen, mit denen Sie den Betriebsstatus Ihres Kontos und Ihrer Ressourcen überprüfen können.

Gelernte Erkenntnisse: Überprüfung und Dokumentation der Reaktion auf Sicherheitsvorfälle, um Verbesserungspotenziale zu identifizieren und als Grundlage für die future Planung der Reaktion auf Vorfälle zu dienen.

Überwachung und Untersuchung: AWS Security Incident Response Überprüft schnell Sicherheitswarnungen von Amazon und stellt die wichtigsten Warnmeldungen GuardDuty, die Ihr Team analysieren muss, in den Vordergrund. Es konfiguriert Unterdrückungsregeln, die auf den Besonderheiten Ihrer Umgebung basieren, um unnötige Warnmeldungen zu vermeiden.

Vorbereitung: Aktivitäten, die unternommen werden, um ein Unternehmen darauf vorzubereiten, effektiv auf Sicherheitsvorfälle zu reagieren und diese zu bewältigen, wie z. B. die Entwicklung von Plänen zur Reaktion auf Zwischenfälle und Testverfahren.

Berichterstattung und Kommunikation: Die Prozesse, mit denen Sie während des gesamten Prozesses zur Reaktion auf Vorfälle auf dem Laufenden gehalten werden, einschließlich automatisierter Benachrichtigungen, Call Bridges und der Bereitstellung von Ermittlungsartefakten. AWS Security Incident Response bietet ein einziges, zentrales Dashboard, über das AWS-Managementkonsole Sie all Ihre AWS Security Incident Response Bemühungen verwalten können.

Von Mitarbeitern generierte Informationen: Indikatoren für Kompromisse, Taktiken, Techniken und Verfahren sowie damit verbundene Muster, die bei AWS Untersuchungen beobachtet wurden.

Fachwissen über Sicherheitsereignisse: Das Fachwissen und die Fähigkeiten, die erforderlich sind, um effektiv auf Sicherheitsereignisse zu reagieren und diese zu bewältigen, insbesondere im Zusammenhang mit der AWS Cloud.

Modell der geteilten Verantwortung: Die Aufteilung der Sicherheitsverantwortung zwischen AWS dem Kunden, wobei der Kunde für die Sicherheit der Cloud verantwortlich AWS ist und der Kunde für die Sicherheit in der Cloud verantwortlich ist.

Bedrohungsinformationen: Interne und externe Datenfeeds mit Informationen zu unbefugten Aktivitäten, um neue Sicherheitsbedrohungen zu identifizieren und darauf zu reagieren.

Ticketsystem: Eine spezielle Fallmanagement-Plattform, mit der Sie Fälle von Sicherheitsereignissen erfassen und verwalten, Anlagen hinzufügen und den Reaktionszyklus auf Vorfälle verfolgen können.

Triage: Die erste Bewertung und Priorisierung eines Sicherheitsereignisses, um die angemessene Reaktion und die nächsten Schritte festzulegen.

Arbeitsablauf: Die festgelegte Abfolge von Schritten und Aktivitäten im Zusammenhang mit der end-to-end Verwaltung eines Sicherheitsereignisses.

Erste Schritte

Erste Schritte mit AWS Security Incident Response

Inhalt

Onboarding-Leitfaden

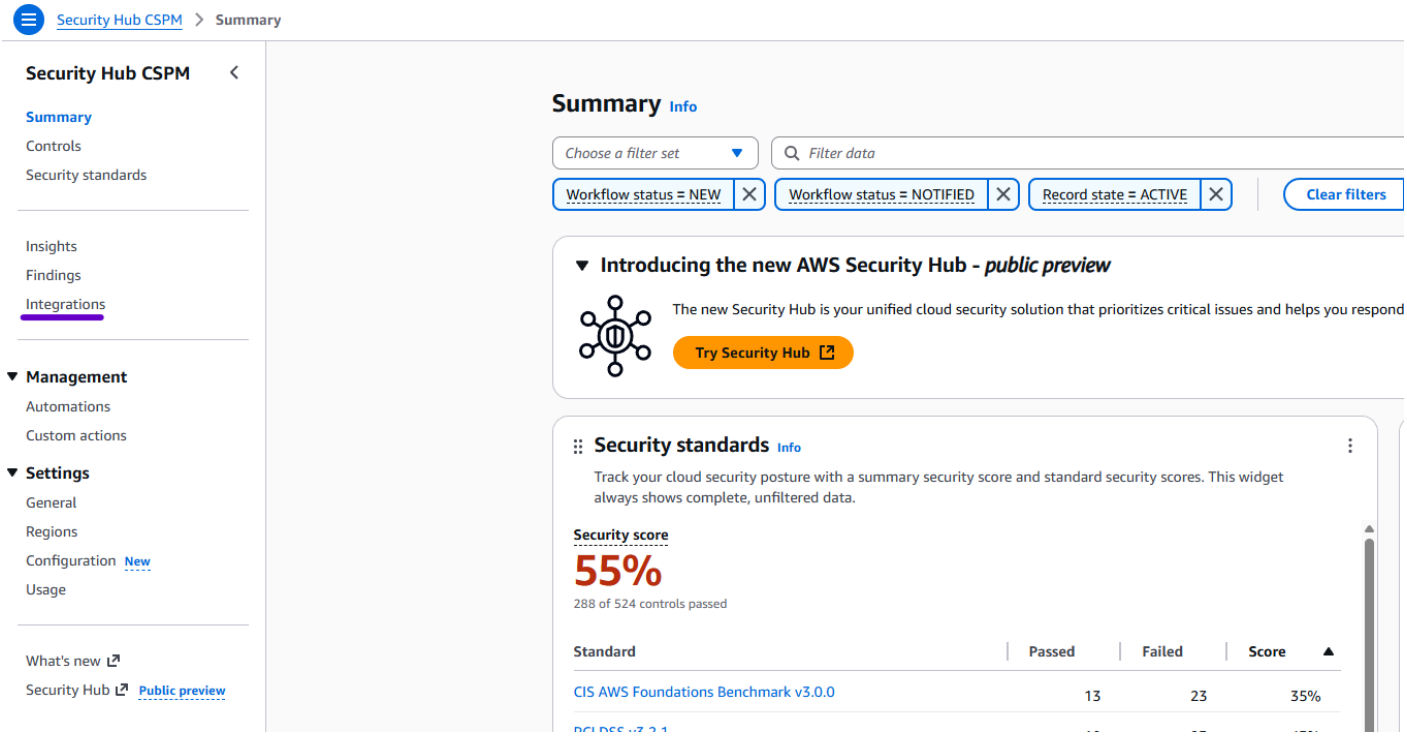
Der Onboarding-Leitfaden führt Sie durch die Voraussetzungen sowie die AWS Security Incident Response Onboarding- und Eindämmungsmaßnahmen.

> **Important**
>
> Voraussetzungen
>
> 1. Die einzige Voraussetzung für die Bereitstellung ist die Aktivierung. AWS Organizations
> 2. Obwohl dies nicht erforderlich ist, empfehlen wir, Amazon GuardDuty und alle Konten zu aktivieren AWS Security Hub CSPMund aktiv AWS-Regionen zu sein, um die Vorteile von Security Incident Response zu maximieren.
> 3. Überprüfung GuardDuty und Reaktion auf Sicherheitsvorfälle.
> 4. Lesen Sie GuardDutyden Leitfaden mit bewährten Methoden.

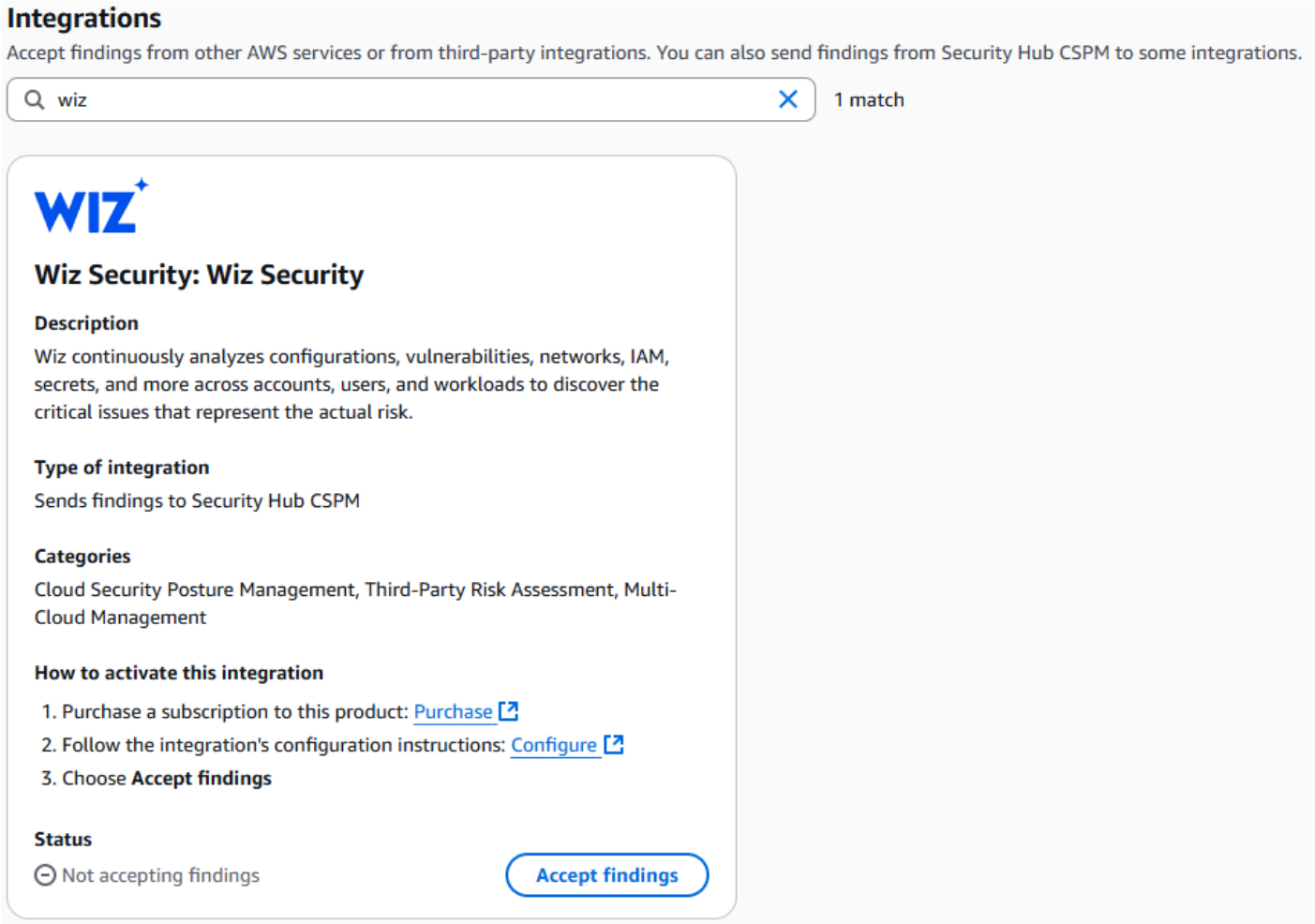
AWS Security Hub CSPM berücksichtigt Ergebnisse von Drittanbietern für Endpoint Detection and Response (EDR) (Endpoint Detection and Response) (CrowdStrikeunter anderem FortinetcNapp (Lacework) und Trend Micro). Wenn diese Ergebnisse in Security Hub CSPM aufgenommen werden, werden sie von Security Incident Response automatisch geprüft, um proaktiv Fälle zu erstellen. Informationen zur Einrichtung von Drittanbieter-EDR mit Security Hub CSPM finden Sie unter Erkennen und Analysieren.

So richten Sie EDR eines Drittanbieters mit Security Hub CSPM ein:

1. Navigieren Sie zur Seite Security Hub CSPM-Integrationen, um zu überprüfen, ob die Drittanbieter-Integration vorhanden ist.
2. Navigieren Sie von der Konsole aus zur Security Hub CSPM-Serviceseite.
3. Wählen Sie Integrationen (am Beispiel von Wiz.io):



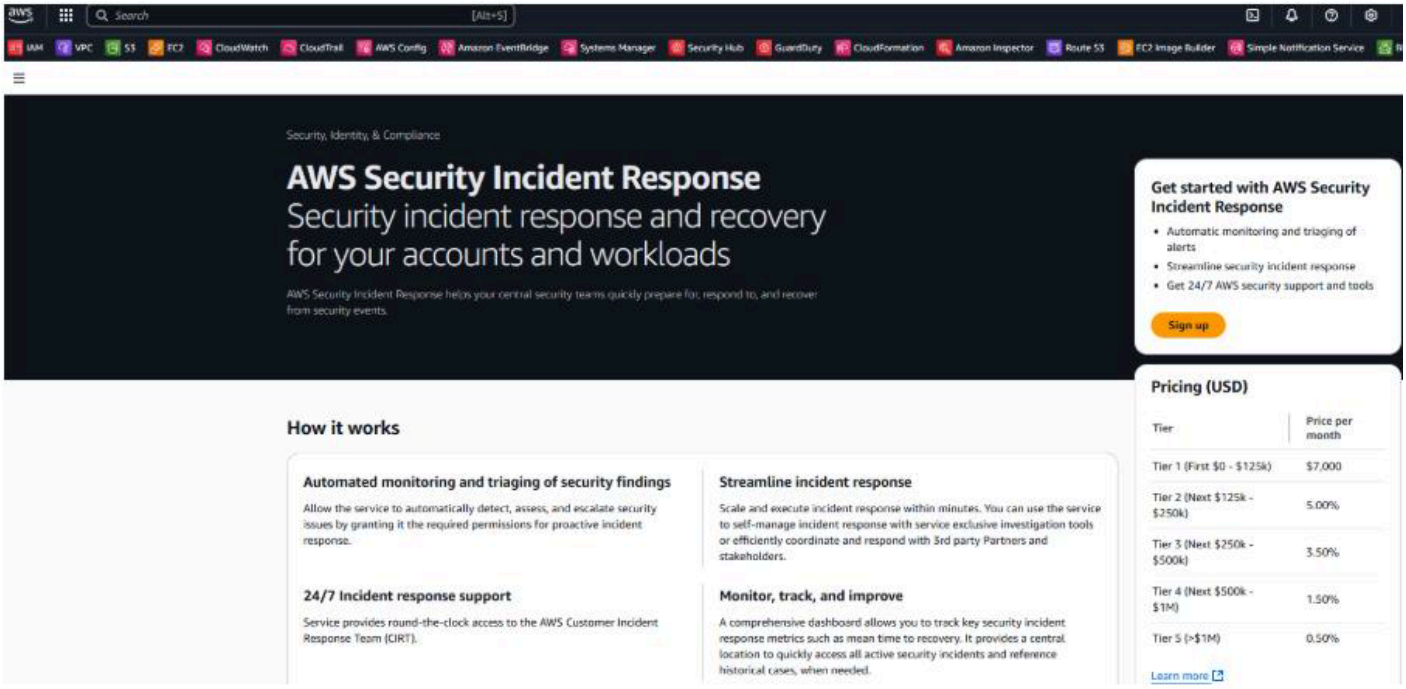
4. Suchen Sie nach dem Anbieter, den Sie integrieren möchten



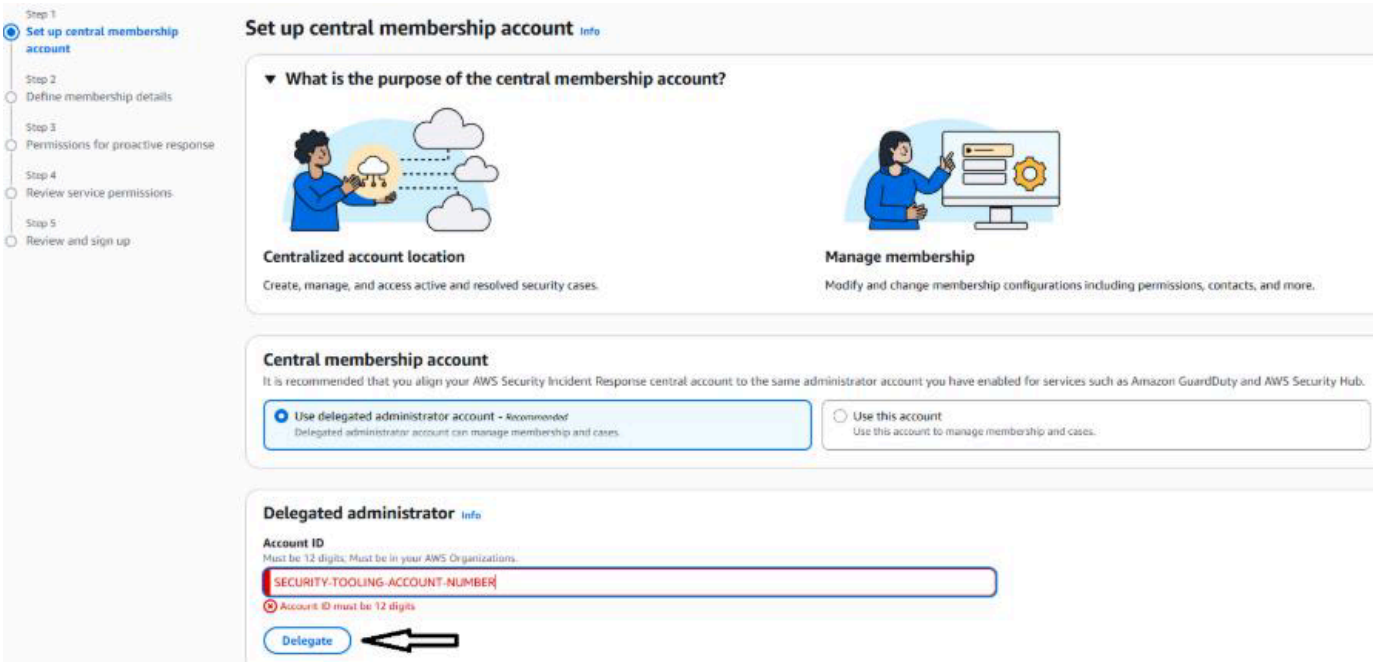
> **Note**
>
> Wenn Sie dazu aufgefordert werden, geben Sie Ihre Konto- oder Abonnementinformationen ein. Nachdem Sie diese Informationen bereitgestellt haben, erfasst Security Incident Response die Ergebnisse von Drittanbietern. Die Preise für die Erfassung von Erkenntnissen durch Dritte finden Sie auf der Seite Integrationen in Security Hub CSPM.

Implementieren und konfigurieren Sie Security Incident Response

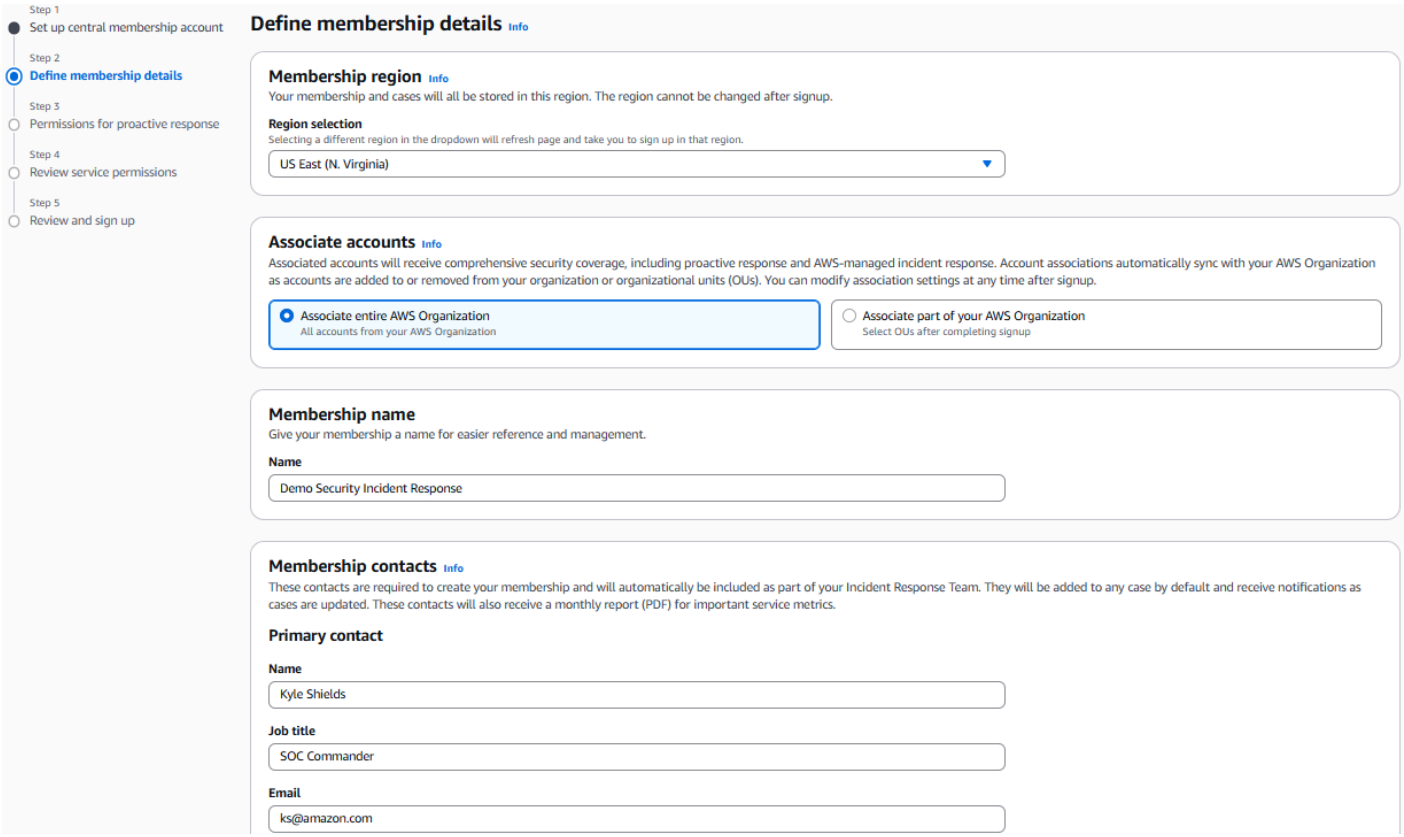
1. Wählen Sie Anmelden



2. Wählen Sie im Verwaltungskonto ein Security-Tooling-Konto als Delegierter Administrator aus.
   - Referenzarchitektur für die Sicherheit
   - Dokumentation für delegierte Administratoren



3. Melden Sie sich beim delegierten Administratorkonto an
4. Geben Sie die Mitgliedsdaten ein und verknüpfen Sie die Konten



Autorisieren Sie Maßnahmen zur Reaktion auf Sicherheitsvorfälle

Auf dieser Seite wird beschrieben, wie Sie Security Incident Response autorisieren, automatisierte Überwachungs- und Eindämmungsmaßnahmen in Ihrer Umgebung durchzuführen. AWS Sie können zwei unterschiedliche Autorisierungsfunktionen aktivieren: proaktive Reaktionsüberwachung und Einstellungen für Eindämmungsmaßnahmen. Diese Funktionen sind unabhängig und können je nach Ihren Sicherheitsanforderungen separat aktiviert werden.

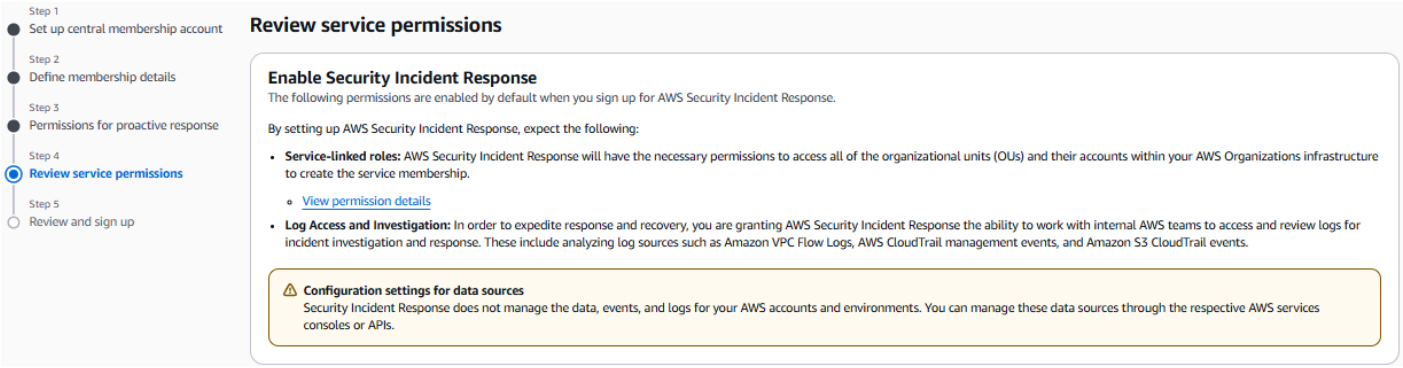
Aktivieren Sie die proaktive Reaktion

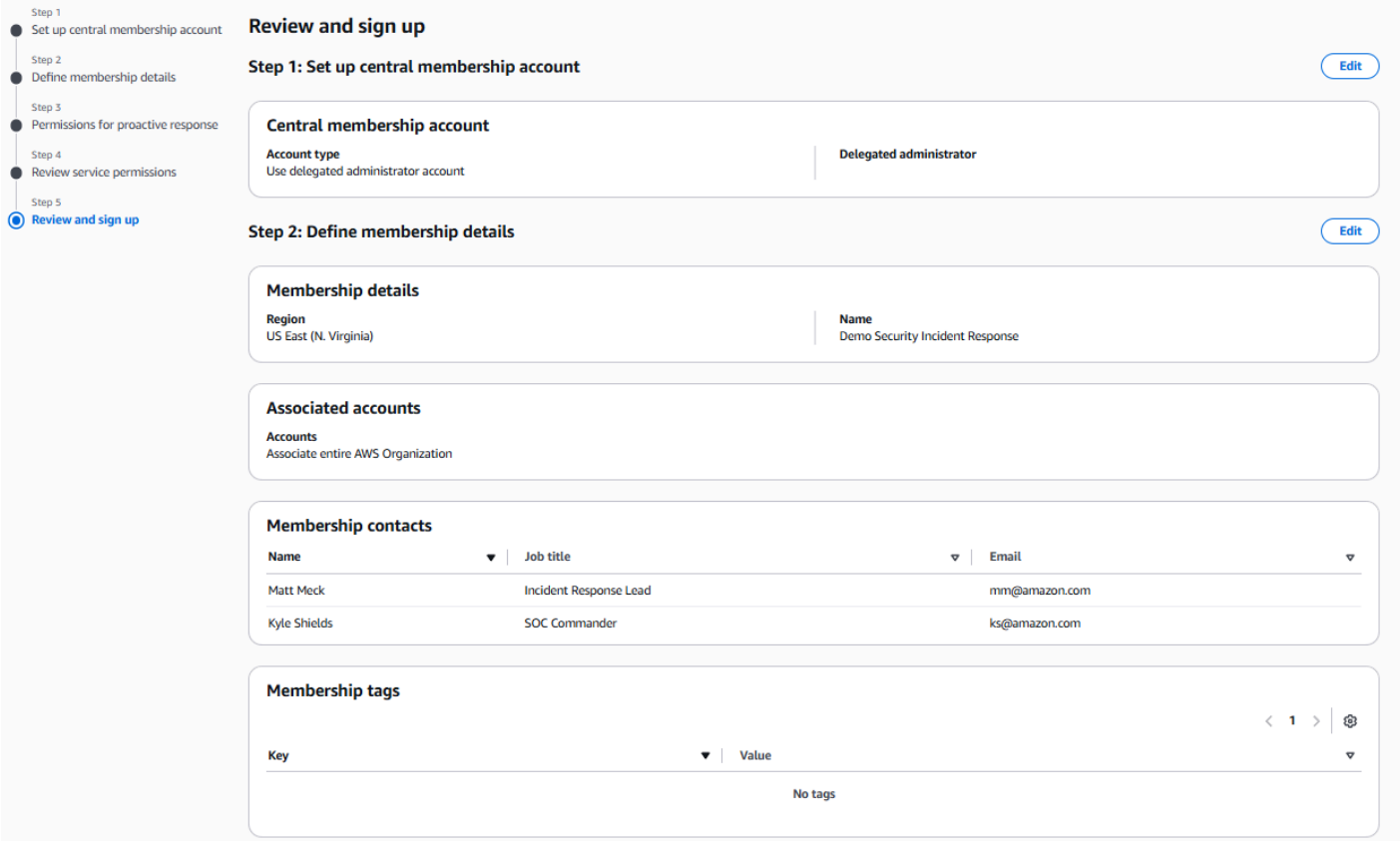
Proactive Response ermöglicht Security Incident Response die Überwachung und Untersuchung von Warnmeldungen, die von Amazon GuardDuty und AWS Security Hub CSPM Integrationen in Ihrem Unternehmen generiert wurden. Wenn diese Option aktiviert ist, sortiert Security Incident Response Warnmeldungen mit niedriger Priorität mithilfe von Serviceautomatisierung aus, sodass sich Ihr Team auf die kritischsten Probleme konzentrieren kann.

Um eine proaktive Reaktion beim Onboarding zu ermöglichen:

1. Navigieren Sie in der Security Incident Response-Konsole zum Onboarding-Workflow.

2. Prüfen Sie die Serviceberechtigungen, die es Security Incident Response ermöglichen, die Ergebnisse aller betroffenen Konten und aktiven Support-Konten AWS-Regionen in Ihrem Unternehmen zu überwachen.
3. Wählen Sie Anmelden, um die Funktion zu aktivieren.





Diese Funktion erstellt automatisch eine dienstbezogene Rolle für alle betroffenen Mitgliedskonten in Ihrem AWS Organizations. Sie müssen die dienstverknüpfte Rolle jedoch manuell im Verwaltungskonto erstellen, indem Sie mit AWS CloudFormation Stack-Sets arbeiten.

Nächste Schritte: Weitere Informationen darüber, wie Security Incident Response mit Amazon GuardDuty funktioniert AWS Security Hub CSPM, finden Sie unter Erkennen und Analysieren im AWS Security Incident Response Benutzerhandbuch.

Definieren Sie die Einstellungen für Eindämmungsmaßnahmen

Eindämmungsmaßnahmen ermöglichen AWS Security Incident Response die Durchführung schneller Reaktionsmaßnahmen während eines aktiven Sicherheitsvorfalls. Diese Maßnahmen tragen dazu bei, die Auswirkungen von Sicherheitsvorfällen in Ihrer Umgebung schnell zu mindern.

> **Important**
>
> Security Incident Response aktiviert standardmäßig keine Eindämmungsfunktionen. Sie müssen Containment-Aktionen in Ihren Containment-Einstellungen ausdrücklich autorisieren.

Um AWS Security Incident Response Techniker zu autorisieren, Containment-Aktionen in Ihrem Namen durchzuführen, müssen Sie zusätzlich zur Bereitstellung eines Systems, AWS CloudFormation StackSetdas die erforderlichen IAM-Rollen erstellt, Ihre Containment-Einstellungen auf Organisations- oder Kontoebene definieren. Einstellungen auf Kontoebene haben Vorrang vor Einstellungen auf Organisationsebene.

Voraussetzungen: Sie müssen über die erforderlichen Berechtigungen verfügen, um Kundenvorgänge zu erstellen. AWS Support

Eindämmungsoptionen:

- Genehmigung erforderlich (Standard): Führen Sie keine proaktive Eingrenzung von Ressourcen ohne ausdrückliche Genehmigung auf einer case-by-case bestimmten Grundlage durch.
- Eingrenzen bestätigt: Führt eine proaktive Eingrenzung einer Ressource durch, bei der bestätigt wurde, dass sie gefährdet ist.
- Verdächtigen Schaden eindämmen: Führen Sie eine proaktive Eingrenzung einer Ressource durch, bei der die Wahrscheinlichkeit, dass sie gefährdet wurde, auf der Grundlage von Analysen, die von Technikern durchgeführt wurden, hoch ist. AWS Security Incident Response

So definieren Sie Containment-Einstellungen:

1. Erstellen Sie einen AWS Support Fall, in dem Sie aufgefordert werden, die Einstellungen für Sicherheitsmaßnahmen für die Reaktion auf Sicherheitsvorfälle zu konfigurieren.

2. Geben Sie in Ihrem Support-Fall Folgendes an:
   - Ihre AWS Organizations ID oder ein bestimmtes Konto, für das IDs Eindämmungsmaßnahmen autorisiert werden sollten
   - Ihre bevorzugte Eindämmungsoption (Genehmigung erforderlich, „Enthalten bestätigt“ oder „Verdachtsfall enthalten“).
   - Die Arten von Containment-Aktionen, die Sie autorisieren möchten (z. B. Isolierung von EC2-Instances, Rotation von Anmeldeinformationen oder Änderungen von Sicherheitsgruppen)
3. AWS Support arbeitet mit Ihnen zusammen, um Ihre Containment-Einstellungen zu konfigurieren. Sie müssen das Notwendige bereitstellen AWS CloudFormation StackSet , um die erforderlichen IAM-Rollen zu erstellen. AWS Support kann bei Bedarf Unterstützung leisten.

Wenn konfiguriert, werden die autorisierten Eindämmungsmaßnahmen bei aktiven Sicherheitsvorfällen AWS Security Incident Response ausgeführt, um Ihre Umgebung zu schützen.

Nächste Schritte: Nachdem die Containment-Einstellungen konfiguriert wurden, können Sie die bei Vorfällen ergriffenen Sicherheitsmaßnahmen in der Security Incident Response-Konsole überwachen.

Nach der Bereitstellung von Security Incident Response

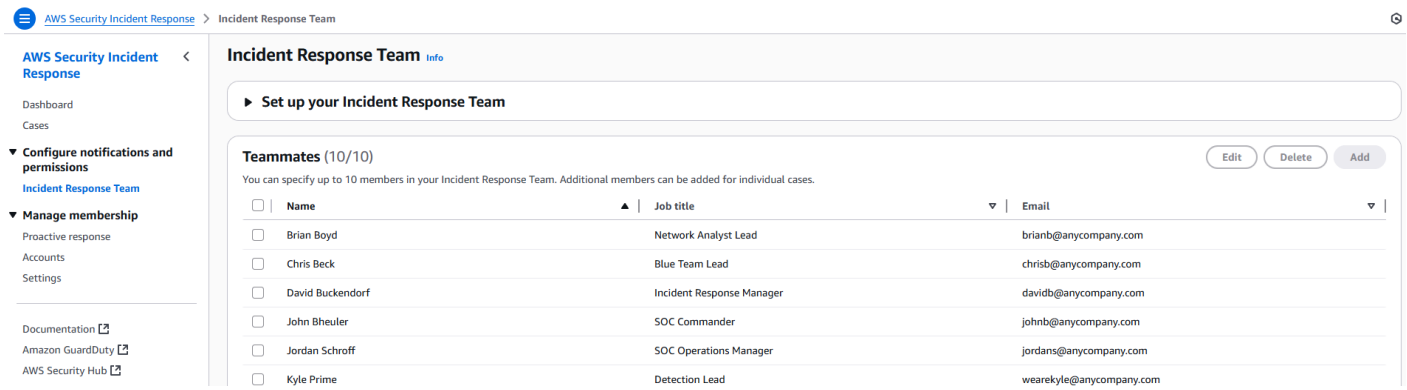
AWS lässt sich in Ihr bestehendes Framework zur Reaktion auf Vorfälle integrieren, anstatt es zu ersetzen.

1. Informieren Sie sich über unsere Möglichkeiten zur betrieblichen Integration, um Ihre aktuellen Verfahren zu verbessern.
2. Sehen Sie sich unsere Demo zur Unterstützung von Mitgliedern auf OU-Ebene, die EventBridge Nutzung und die Jira-ITSM-Integration für effizientere Sicherheitsabläufe an.

   AWS Security Incident Response: Neue Integrationen und Abonnement auf OU-Ebene

Informieren Sie das Incident Response Team

1. Vergewissern Sie sich, dass Sie abonniert sind und die in diesem Onboarding-Leitfaden beschriebenen Onboarding-Schritte abgeschlossen haben.
2. Wählen Sie in der linken Navigationsleiste Incident Response Team aus.
3. Wählen Sie die Teammitglieder aus, die Sie Ihrem Team hinzufügen möchten.



> **Note**
>
> Das Team kann aus Unternehmensleitern, Rechtsberatern, MDR-Partnern, Cloud-Ingenieuren und anderen bestehen. Sie können bis zu 10 weitere Mitglieder hinzufügen. Geben Sie für jedes Mitglied nur Name, Titel und E-Mail-Adresse an.

AWS unterstützter Fall

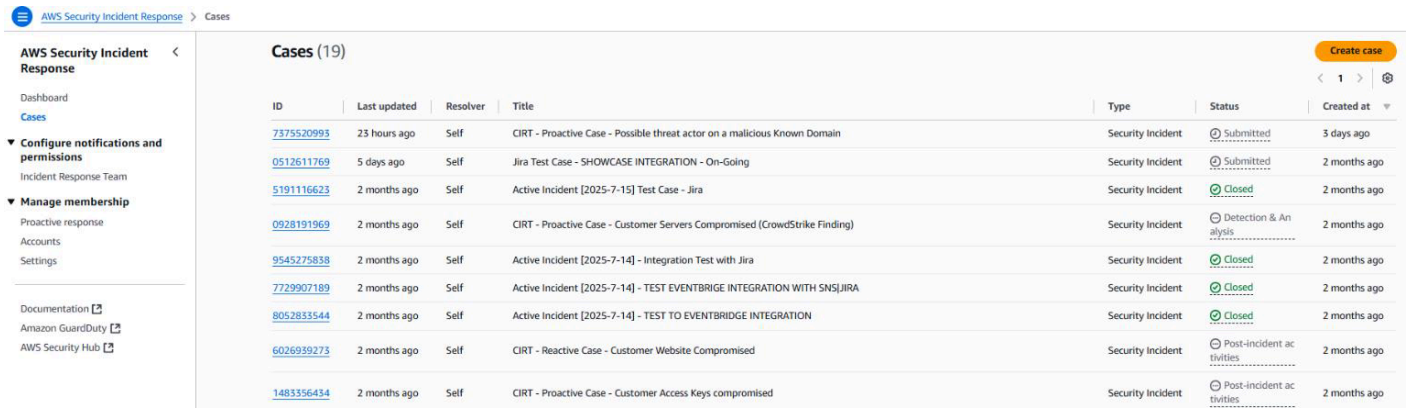
AWS Security Incident Response bietet ein abonnementbasiertes Fallmanagement-Portal, über das Ihr Unternehmen direkt mit unseren Security Incident Response-Technikern Kontakt aufnimmt. Wir unterstützen Sie bei Sicherheitsuntersuchungen und aktiven Vorfällen mit einem SLO von 15 Minuten, ohne Beschränkung auf reaktive Fälle. Weitere Informationen finden Sie in unserer Dokumentation „Einen AWS unterstützten Fall erstellen“.

Erweitern Sie das Ermittlungsteam

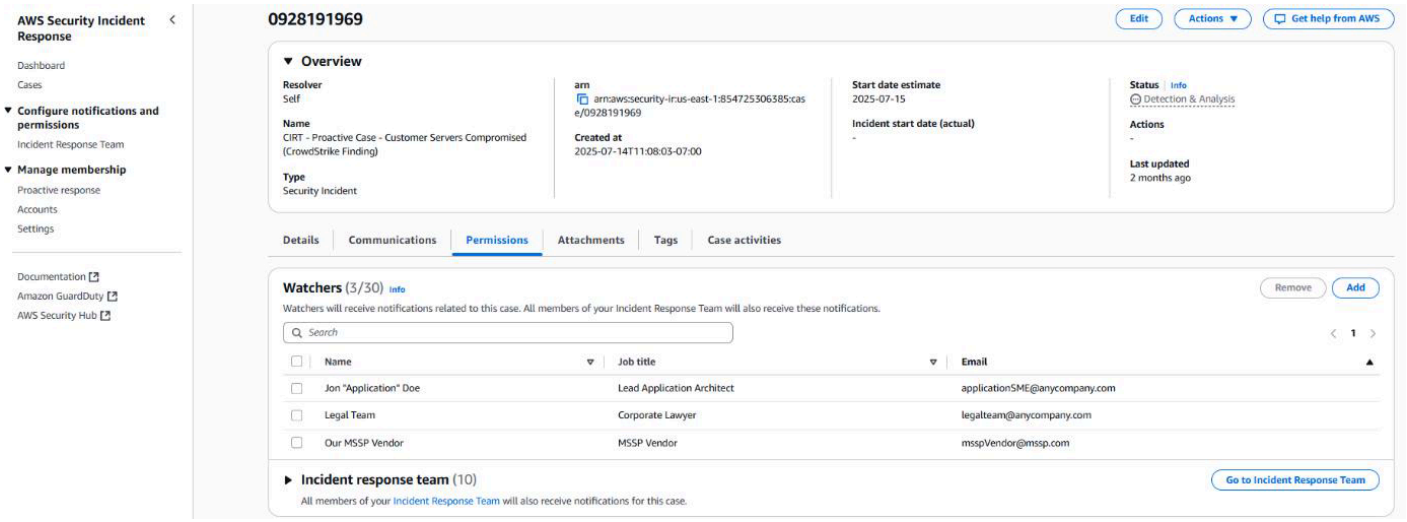
Über das Case Management Portal können Sie externen Parteien Einblick in den Fall gewähren, indem Sie Beobachter- und IAM-Richtlinien hinzufügen. Nutzen Sie diese Optionen für Partner, Rechtsteams oder Fachexperten.

So fügen Sie Beobachter zu einem Fall hinzu:

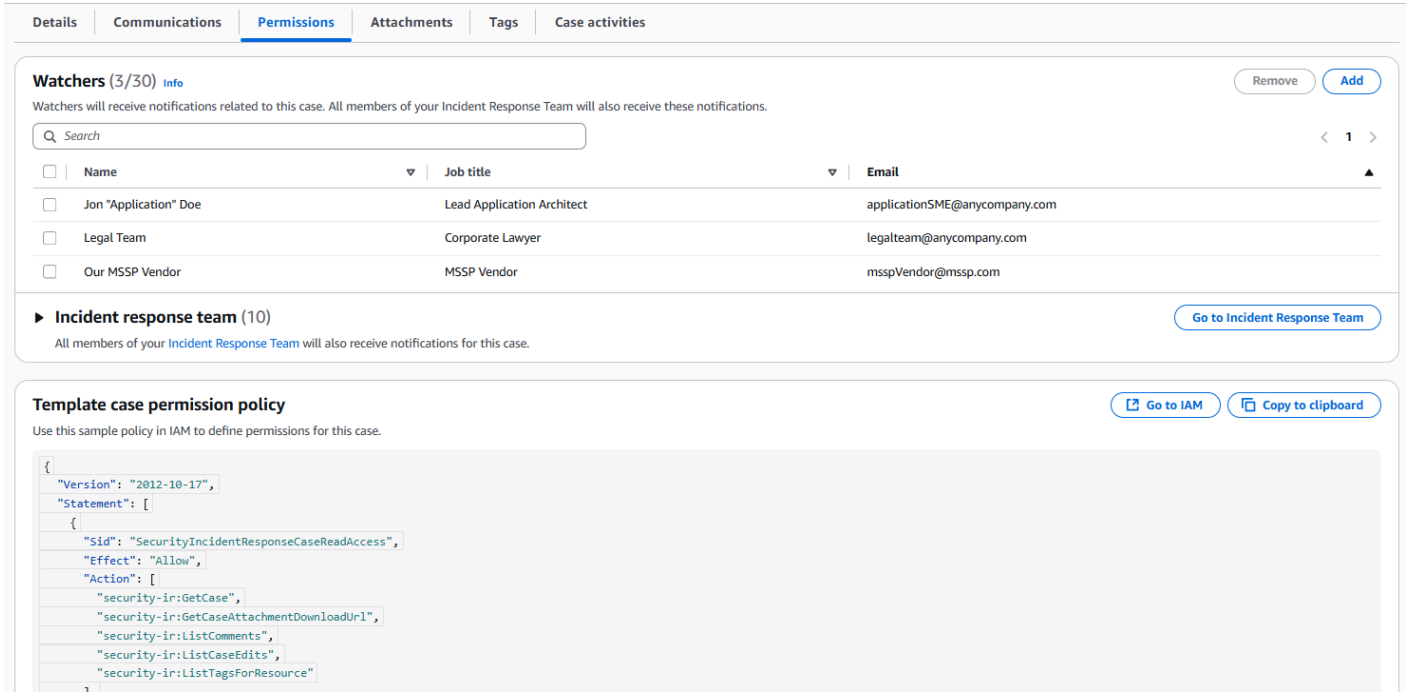
1. Öffnen Sie einen beliebigen Fall über das Security Incident Response Cases Portal.



2. Wählen Sie die Registerkarte „Berechtigungen“



3. Wählen Sie Hinzufügen



> **Note**
>
> Jeder Fall beinhaltet eine vorab ausgefüllte IAM-Richtlinie, die nur für diesen speziellen Fall Zugriff gewährt, wobei die geringsten Rechte beibehalten werden. Kopieren Sie diese Richtlinie und fügen Sie sie direkt in die IAM-Rollen oder -Benutzer von Drittanbietern oder bestimmten Ermittlungsteams ein, um deren Beitrag zu ermöglichen.

GuardDuty Feststellungen und Regeln zur Unterdrückung

AWS Security Incident Response nimmt proaktiv alle Ergebnisse und GuardDuty AWS Security Hub CSPM Ergebnisse von Amazon, FortinetcNapp (Lacework) und Trend Micro auf CrowdStrike, bewertet sie und reagiert darauf. Unsere Auto-Triage-Technologie macht interne Analyseanforderungen überflüssig. Der Dienst erstellt Regeln zur Unterdrückung und automatischen Archivierung in GuardDuty Security Hub CSPM für harmlose Ergebnisse. Sehen Sie sich diese Regeln in der GuardDuty Amazon-Konsole unter „Ergebnisse“ an oder ändern Sie sie.

Gehen Sie wie folgt vor, um die aktivierten GuardDuty Unterdrückungsregeln zu überprüfen:

1. Öffnen Sie die GuardDuty Amazon-Konsole.
2. Wählen Sie Findings aus.
3. Wählen Sie im Navigationsbereich die Option Unterdrückungsregeln aus. Auf der Seite mit den Unterdrückungsregeln wird eine Liste aller Unterdrückungsregeln für Ihr Konto angezeigt.
4. Um die Einstellungen für eine Regel zu überprüfen oder zu ändern, wählen Sie die Regel aus und klicken Sie dann im Menü Aktionen auf Unterdrückungsregel aktualisieren.

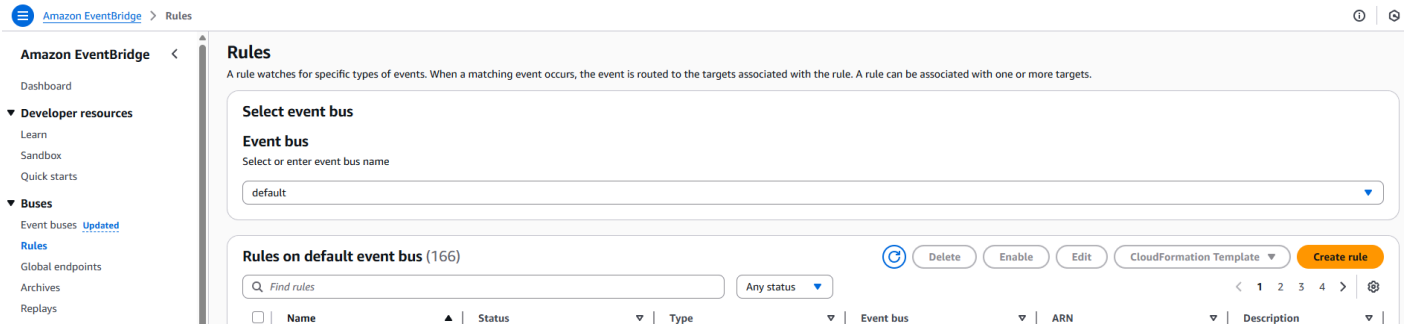
> **Note**
>
> Organizations, die SIEM-Technologie einsetzen, haben im Laufe der Zeit das GuardDuty Fundvolumen erheblich reduziert und damit sowohl den Security Incident Response-Service als auch die SIEM-Effizienz verbessert.

Amazon EventBridge

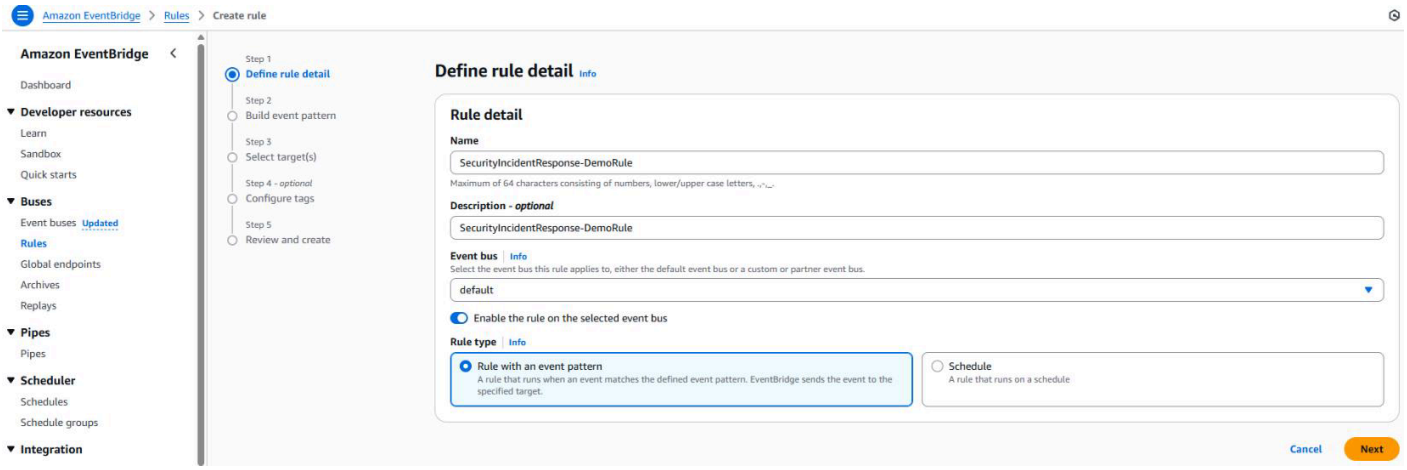
Amazon EventBridge ermöglicht eine ereignisgesteuerte Architektur für Security Incident Response, sodass Fallaktivitäten nachgelagerte Dienste (SNS, Lambda, SQS, Step-Functions) oder externe Tools (Jira, Teams, Slack,) auslösen können. ServiceNow PagerDuty

So konfigurieren Sie Regeln: EventBridge

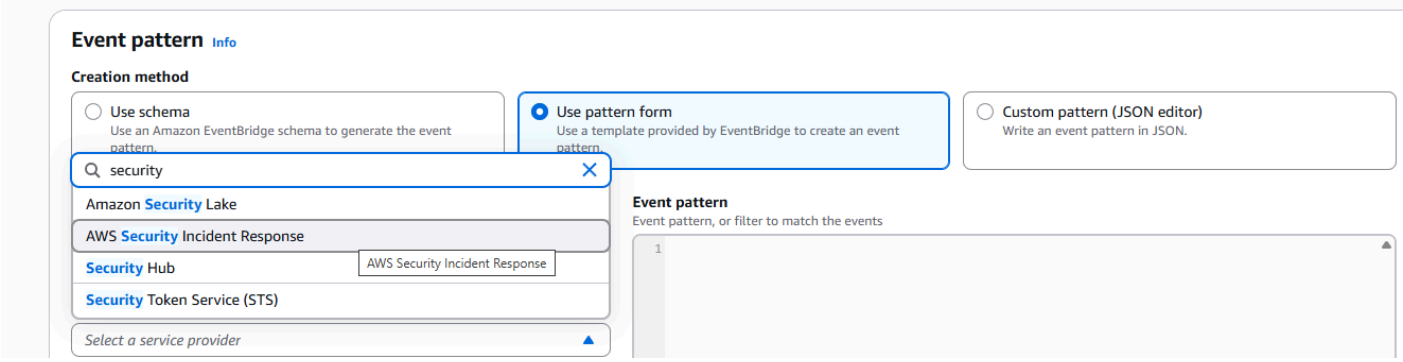
1. Zugriff auf Amazon EventBridge
2. Wählen Sie im Drop-down-Menü Busse die Option Regeln aus.



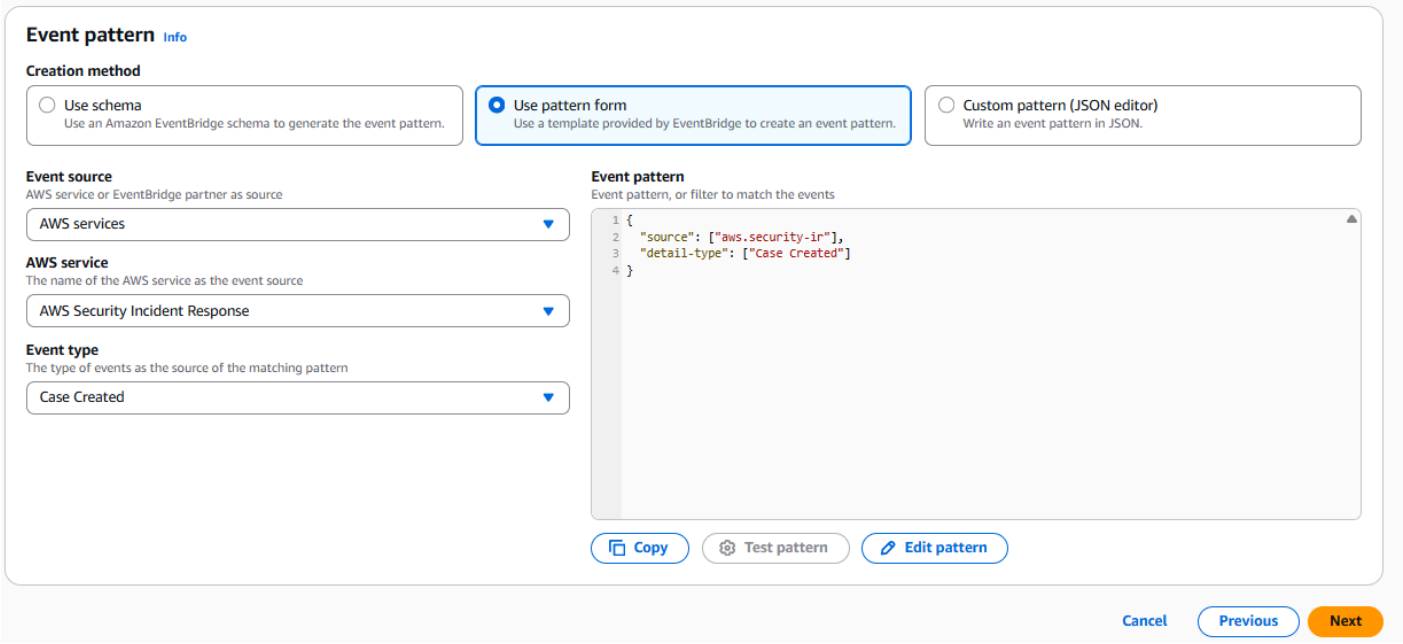
3. Wählen Sie Create Rule (Regel erstellen) aus.
4. Geben Sie die Regeldetails ein.
5. Wählen Sie Weiter aus.



6. Scrollen Sie zu AWS Service,. und wählen Sie dann AWS Security Incident Responseaus dem Dropdownmenü aus.

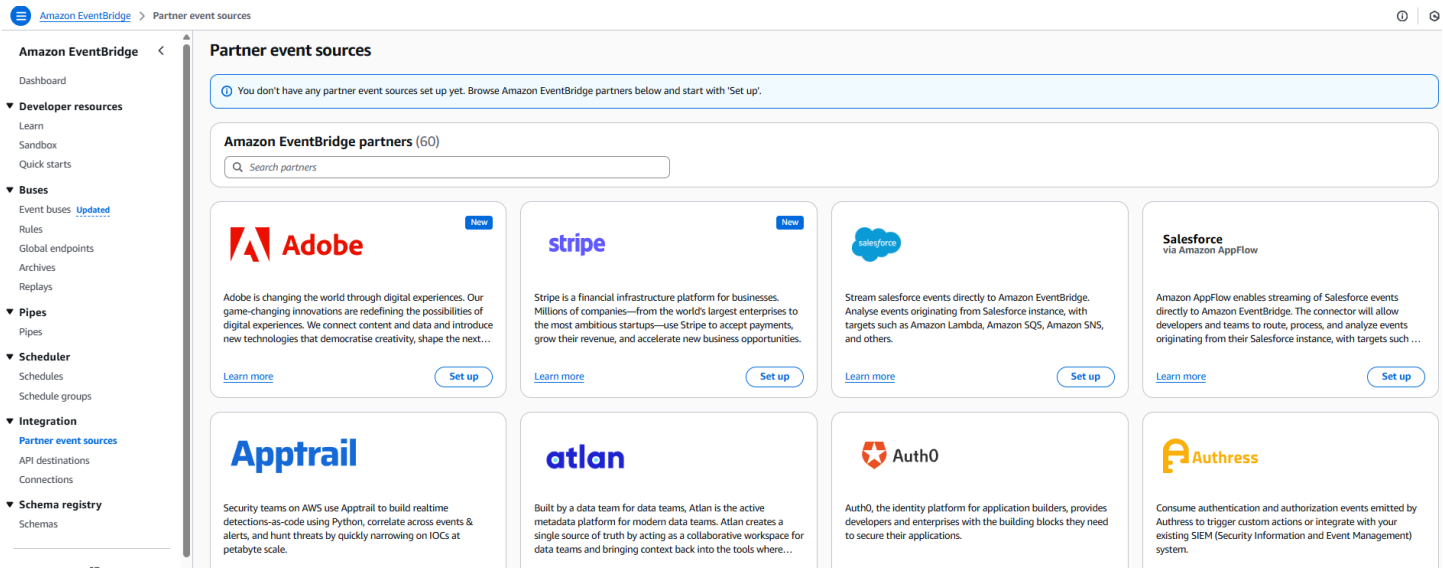


7. Wählen Sie in der Dropdownliste Ereignistyp das Ereignis oder den API-Aufruf aus, für den Sie ein Muster erstellen möchten.
8. Sie können das Muster manuell bearbeiten, um mehr als ein Ereignis einzubeziehen.
9. Wählen Sie Weiter aus.



> **Note**
>
> Wählen Sie ein oder mehrere Ziele (Amazon Simple Notification Service AWS Lambda, SSM-Dokument, Step-Function) für Ihre Ereignisse aus. Konfigurieren Sie bei Bedarf kontenübergreifende Ziele.

Sie können im Integrationsmenü unter Partnerereignisquellen nach Mustern bei der EventBridge Partnerintegration suchen. Zu den verfügbaren Partnern gehören unter anderem Atlassian (Jira) DataDog, New Relic PagerDuty, Symantec und Zendesk.



Integrationen und Workflow für externe Tools

AWS Lösungen zur Integration von JIRA oder ServiceNow mit Security Incident Response

Stellen Sie unsere voll entwickelten Lösungen für die bidirektionale Integration mit Jira und bereit. ServiceNow Diese Integrationen ermöglichen eine bidirektionale Kommunikation zwischen AWS Security Incident Response Fällen und Ihrer ITSM-Plattform, wobei Fallaktualisierungen automatisch in den entsprechenden Jira-Aufgaben berücksichtigt werden.

Vorteile der Integration

Durch die AWS Security Incident Response Integration in Ihre bestehende ITSM-Plattform werden Ihre Sicherheitsabläufe optimiert, indem die Workflows zur Nachverfolgung und Reaktion auf Vorfälle zentralisiert werden. Diese vorgefertigten Lösungen machen eine kundenspezifische Entwicklung überflüssig und ermöglichen es Ihren Sicherheitsteams, den Überblick sowohl über AWS native als auch über unternehmensweite Incident-Management-Systeme zu behalten. Durch die Nutzung von Amazon EventBridge für die ereignisgesteuerte Automatisierung werden Updates nahtlos und in Echtzeit zwischen den Plattformen ausgetauscht. Dadurch wird sichergestellt, dass Sicherheitsvorfälle unabhängig von ihrem Ursprung konsistent verfolgt werden. Dieser einheitliche Ansatz reduziert den Kontextwechsel für Sicherheitsanalysten, verbessert die Reaktionszeiten und bietet umfassende Prüfprotokolle für Ihren gesamten Reaktionszyklus auf Vorfälle.

So konfigurieren Sie EventBridge Regeln:

1. Greifen Sie auf Amazon EventBridge zu.
2. Wählen Sie im Drop-down-Menü Busse die Option Regeln aus.

Arbeitsablauf bei der externen Werkzeugausstattung

Security Incident Response lässt sich auf vielfältige Weise in externe Tools und Partner integrieren:

- SIEM-Integration: Die Security Incident Response-Techniker helfen Ihnen, diese Ergebnisse parallel mit Ihrem Team zu analysieren und zu untersuchen, wenn Sie AWS unterstützte Fälle einreichen. Wir identifizieren Zusammenhänge zwischen Hybrid- und Multi-Cloud-Umgebungen und helfen so, die Bewegungen von Bedrohungsakteuren zwischen Anbietern einzuschätzen.
- Verbessert Ihre bestehenden Sicherheitsabläufe: Wir ersetzen herkömmliche GuardDuty Reaktionsabläufe durch ein effizienteres, paralleles Reaktionsmodell. Viele Unternehmen nutzen derzeit SIEM-Technologie für Erkennungsworkflows im Rahmen des Fallmanagements. Dieser Service bietet eine optimierte Alternative speziell für GuardDuty (und ausgewählte Security Hub CSPM) Ergebnisse. Die Lösung nutzt ausgefeilte Auto-Triage-Technologie mit menschlicher Aufsicht, um proaktive Fälle in Ihrem Portal zu erstellen, gleichzeitig Ihr Reaktionsteam zu benachrichtigen und unsere Security Incident Response Engineers mit koordinierten Abhilfemaßnahmen zu beauftragen.
- Ermittlungsteams von Drittanbietern: Unsere Security Incident Response Engineers arbeiten direkt mit Ihren Partnern und MDR-Anbietern zusammen.

Anhang A: Ansprechpartner

Wenn Sie Ihre Metadaten im Voraus unseren Security Incident Response-Technikern zur Verfügung stellen, kann dies dazu beitragen, die Profilerstellung zu beschleunigen und das Vertrauen in unsere Triaging-Technologie von Anfang an zu stärken. Dies trägt dazu bei, die Anzahl von Fehlalarmen zu reduzieren, die im Vorfeld festgestellt werden, wenn wir damit beginnen, Ihre Bedrohungserkenntnisse zu erfassen und Ihre „bekanntermaßen gute Welt“ zu schaffen.

Kontaktinformationen für IR- und SOC-Mitarbeiter

Ein	IR | SOC-Personal: Rolle, Name, E-Mail	Primä und sekun Anspr artner für Eskal nen	Intern bekan CIDR-Bere iche	Extern bekan CIDR-Bere iche	Zusät he Cloud Die nstanl er	AWS Arbeit gioner	DNS-Serve r IPs (falls nicht Amaz Route 53 Resol	VPN | Fernzug ffslösun en und IPs	Kritische Anwend snamen | Kontonu ern	Häufig verwe e ungev iche Ports	EDR | AV | Verwend e Tools für das Schwacl ellenma gement	IDP | Standorte
1	SOC-Komma ndeur, John Smith, jsmith@ ample.c	Prima	10.0.0 16	5.5.60 20 (Azurl)	Azure	us-east-1 , us-east-2	–	Direktve bindung öffentlic he VIF 116.32.8 7	Nginx Webserv (Beispie kritisch) | 1234567 0	8080	CrowdSt ke Falcon	Entra, Azure

Um Metadateninformationen für Ihre Umgebung einzureichen, erstellen Sie einen AWS Support Fall.

Um Metadaten einzureichen

1. Füllen Sie die Metadatentabelle mit Ihren Umgebungsinformationen aus.
2. Erstellen Sie einen AWS Support Fall mit den folgenden Details:
   - Art des Falls: Technisch
   - Service: Service zur Reaktion auf Sicherheitsvorfälle
   - Kategorie: Andere
3. Hängen Sie die ausgefüllte Metadatentabelle an den Fall an.

RACI-Matrix

Die folgende RACI-Matrix definiert Rollen und Verantwortlichkeiten im gesamten Implementierungsprozess von Security Incident Response. RACI steht für Responsible (R), Accountable (A), Consulted (C) und Informed (I).

Aktivität	Customer	AWS Kundenbetreuungsteam	SIR-Mannschaft
Vor dem Onboarding			
Identifizieren Sie die wichtigsten Stakeholder	R		I
Bestätigen Sie die Suche nach Quellen	R	C	I
[EDR-Integration von Drittanbietern] Security Hub CSPM	R	C	I
GuardDuty Validierung/Gesundheitscheck	C	R	I
Ermitteln Sie den Kontobereich	R		
Eskalationsprotokolle einrichten	R	I	C
AWS Organizations aktivieren	R	C	
Ordnen Sie Konten zu AWS Organizations	R	I	
Wählen Sie Delegated Administrator/ Security Tooling-Konto aus	R	I	
Onboarding			
Einzelheiten zur Mitgliedschaft einrichten	R	I	

Aktivität	Customer	AWS Kundenbetreuungsteam	SIR-Mannschaft
Exemplarische Vorgehensweise (Einrichtung proaktiver Workflows für Reaktion und Alert-Triaging; Bereitstellung einer serviceverknüpften Rolle für das Verwaltungskonto; Autorisieren von Eindämmungsaktionen)	R	C	I
Konfiguration nach der Bereitstellung			
Überprüfen Sie die betrieblichen Integrationsmöglichkeiten	R	C	I
Reichen Sie reaktive Fälle zur Reaktion auf Sicherheitsvorfälle ein	R		
EventBridge Amazon-Integrationen konfigurieren	R	C	C
Connect Tools von Drittanbietern (Jira, ServiceNow, PagerDuty, Teams usw.)	R	I	C
Tiefer Einblick in den Service und Demo	A	R	C

RACI-Definitionen:

- Verantwortlich (R) — Die Partei, die die Arbeit zur Erledigung der Aufgabe ausführt
- Verantwortlich (A) — Die Partei, die letztendlich für die korrekte Ausführung der Aufgabe verantwortlich ist
- Konsultiert (C) — Die Partei, deren Meinung eingeholt wird und mit der eine wechselseitige Kommunikation besteht
- Informiert (I) — Die Partei, die up-to-date auf dem Laufenden gehalten wird und mit der eine einseitige Kommunikation besteht

Wählen Sie ein Mitgliedskonto

Ein Mitgliedskonto ist das AWS Konto, das verwendet wird, um Kontodetails zu konfigurieren, Details für Ihr Incident-Response-Team hinzuzufügen und zu entfernen und in dem alle aktiven und historischen Sicherheitsereignisse erstellt und verwaltet werden können. Es wird empfohlen, dass Sie Ihr AWS Security Incident Response Mitgliedskonto demselben Konto zuordnen, das Sie für Dienste wie Amazon GuardDuty und aktiviert haben AWS Security Hub CSPM.

Sie haben zwei Möglichkeiten, Ihr AWS Security Incident Response Mitgliedskonto auszuwählen AWS Organizations. Sie können entweder eine Mitgliedschaft im Verwaltungskonto für Organizations oder in einem delegierten Administratorkonto für Organizations erstellen.

Verwenden Sie das delegierte Administratorkonto: AWS Security Incident Response Verwaltungsaufgaben und die Fallverwaltung befinden sich im delegierten Administratorkonto. Wir empfehlen, denselben delegierten Administrator zu verwenden, den Sie für andere AWS Sicherheits- und Compliance-Dienste eingerichtet haben. Geben Sie die 12-stellige ID des delegierten Administratorkontos ein und melden Sie sich dann bei diesem Konto an, um fortzufahren.

Important

Wenn Sie im Rahmen der Installation ein delegiertes Administratorkonto verwenden, AWS Security Incident Response kann die erforderliche verknüpfte Rolle mit dem Triage-Service nicht automatisch in Ihrem Verwaltungskonto erstellt werden. AWS Organizations
Sie können das IAM verwenden, um diese Rolle in Ihrem Verwaltungskonto zu erstellen AWS Organizations

So erstellen Sie eine serviceverknüpfte Rolle (Konsole)

1. Loggen Sie sich in Ihr AWS Organizations Verwaltungskonto ein.
2. Greifen Sie mit Ihrer bevorzugten Methode über CLI auf das AWS CloudShellFenster zu oder greifen Sie auf das Konto zu.
3. Verwenden Sie den CLI-Befehl `aws iam create-service-linked-role --aws-service-name "triage.security-ir.amazonaws.com" --no-cli-pager`
4. (Optional) Um zu überprüfen, ob der Befehl funktioniert hat, können Sie den Befehl ausführen `aws iam get-role --role-name AWSServiceRoleForSecurityIncidentResponse_Triage`

Verwenden Sie das aktuell angemeldete Konto: Wenn Sie dieses Konto auswählen, wird das aktuelle Konto als zentrales Mitgliedskonto für Ihre AWS Security Incident Response Mitgliedschaft bestimmt. Einzelpersonen in Ihrer Organisation müssen über dieses Konto auf den Service zugreifen, um aktive und gelöste Fälle zu erstellen, darauf zuzugreifen und diese zu verwalten.

Stellen Sie sicher, dass Sie über ausreichende Verwaltungsberechtigungen verfügen. AWS Security Incident Response

Spezifische Schritte zum Hinzufügen von Berechtigungen finden Sie unter Hinzufügen und Entfernen von IAM-Identitätsberechtigungen.

Weitere Informationen finden Sie unter AWS Security Incident Response Verwaltete Richtlinien.

Gehen Sie wie folgt vor, um IAM-Berechtigungen zu überprüfen:

- Überprüfen Sie die IAM-Richtlinie: Überprüfen Sie die Ihrem Benutzer, Ihrer Gruppe oder Rolle zugeordnete IAM-Richtlinie, um sicherzustellen, dass sie die erforderlichen Berechtigungen gewährt. Sie können dies tun, indem Sie zu der navigieren https://console.aws.amazon.com/iam/, die `Users` Option auswählen, den jeweiligen Benutzer auswählen und dann auf der Übersichtsseite zu der `Permissions` Registerkarte wechseln, auf der Sie eine Liste aller angehängten Richtlinien sehen können. Sie können jede Richtlinienzeile erweitern, um deren Details anzuzeigen.
- Testen Sie die Berechtigungen: Versuchen Sie, die Aktion auszuführen, die Sie zur Überprüfung der Berechtigungen benötigen. Wenn Sie beispielsweise auf einen Fall zugreifen müssen, versuchen Sie es`ListCases`. Wenn Sie nicht über die erforderlichen Berechtigungen verfügen, erhalten Sie eine Fehlermeldung.
- Verwenden Sie das SDK AWS CLI oder ein SDK: Sie können das AWS Command Line Interface oder ein AWS SDK in Ihrer bevorzugten Programmiersprache verwenden, um die Berechtigungen zu testen. Mit dem können Sie beispielsweise den `aws sts get-caller-identity` Befehl ausführen AWS Command Line Interface, um Ihre aktuellen Benutzerberechtigungen zu überprüfen.
- Überprüfen Sie die AWS CloudTrail Protokolle: Überprüfen Sie die CloudTrail Protokolle, um festzustellen, ob die Aktionen, die Sie ausführen möchten, protokolliert werden. Dies kann Ihnen helfen, etwaige Probleme mit Berechtigungen zu identifizieren.
- Verwenden Sie den IAM-Richtliniensimulator: Der IAM-Richtliniensimulator ist ein Tool, mit dem Sie IAM-Richtlinien testen und feststellen können, welche Auswirkungen sie auf Ihre Berechtigungen haben.

> **Note**
>
> Die spezifischen Schritte können je nach AWS Service und den Aktionen, die Sie ausführen möchten, variieren.

Einzelheiten zur Mitgliedschaft einrichten

- Wählen Sie einen AWS-Region Ort aus, an dem Ihre Mitgliedschaft und Ihre Fälle gespeichert werden sollen.

  > **Warning**
  >
  > Sie können die Standardeinstellung AWS-Region nach der ersten Registrierung der Mitgliedschaft nicht ändern.

- Wählen Sie aus, ob Sie Ihre gesamte Mitgliedschaft oder einen Teil Ihrer AWS Organizations Organisationseinheiten vollständig AWS Organizations oder teilweise abdecken möchten (OUs).
- Sie können optional einen Namen für diese Mitgliedschaft wählen.
- Im Rahmen des Workflows zum Erstellen einer Mitgliedschaft müssen ein primärer und ein sekundärer Kontakt angegeben werden. Diese Kontakte werden automatisch in Ihr Incident-Response-Team aufgenommen. Für eine einzelne Mitgliedschaft müssen mindestens zwei Kontakte vorhanden sein, wodurch auch sichergestellt wird, dass mindestens zwei Kontakte zum Incident-Response-Team gehören.
- Definieren Sie optionale Tags für Ihre Mitgliedschaft. Mithilfe von Tags können Sie die AWS Kosten verfolgen und nach Ressourcen suchen.

Ordnen Sie Konten zu AWS Organizations

Wenn Sie sich AWS Organizations bei der Einrichtung dafür entschieden haben, Ihr gesamtes Konto zuzuordnen, gilt Ihre Mitgliedschaft für alle Mitgliedskonten in der Organisation. Zugeordnete Konten werden automatisch aktualisiert, wenn Konten zu Ihrer Organisation hinzugefügt oder daraus entfernt werden.

Wenn Sie sich AWS Organizations bei der Einrichtung dafür entschieden haben, einen Teil Ihrer Konten zuzuordnen, und Ihre Mitgliedschaft auf bestimmte Organisationseinheiten (OUs) beschränkt haben, gilt Ihre Mitgliedschaft für alle Konten unter den ausgewählten OUs Konten. Dies schließt

Konten ein, die zu den ausgewählten OUs Konten gehören. OUs Zugeordnete Konten werden automatisch aktualisiert, wenn Konten hinzugefügt oder daraus entfernt werden OUs.

Weitere Informationen zu bewährten Methoden im Zusammenhang mit Organisationseinheiten finden Sie unter Organisieren Ihrer AWS Umgebung mithilfe mehrerer Konten.

Richten Sie proaktive Reaktions- und Alert-Triaging-Workflows ein

AWS Security Incident Response überwacht und untersucht Bedrohungswarnungen, die von den CSPM-Integrationen von Amazon GuardDuty und Security Hub generiert wurden. Um diese Funktion nutzen zu können, GuardDuty muss Amazon aktiviert sein. AWS Security Incident Response sortiert Warnmeldungen mit niedriger Priorität mithilfe von Serviceautomatisierung aus, sodass sich Ihr Team auf die kritischsten Probleme konzentrieren kann. Weitere Informationen zur AWS Security Incident Response Funktionsweise mit Amazon GuardDuty und AWS Security Hub CSPM finden Sie im Abschnitt Erkennen und Analysieren des Benutzerhandbuchs.

Wenn Sie Probleme beim Onboarding haben, erstellen Sie einen AWS Support Fall für zusätzliche Unterstützung. Stellen Sie sicher, dass Sie Details wie die AWS-Konto ID und alle Fehler angeben, die Ihnen während des Einrichtungsvorgangs möglicherweise aufgefallen sind.

> **Note**
>
> Wenn Sie Fragen zu GuardDuty Amazon-Unterdrückungsregeln, Alert-Triaging-Konfigurationen oder proaktiven Reaktionsabläufen haben, können Sie einen AWS unterstützten Fall mit dem Falltyp Ermittlungen und Anfragen erstellen und sich an das Team für die Reaktion auf AWS Sicherheitsvorfälle wenden. Weitere Informationen finden Sie unter Erstellen Sie einen AWS unterstützten Fall.

Mit dieser Funktion können AWS Security Incident Response Sie die Ergebnisse aller betroffenen Konten und aktiven unterstützten AWS Regionen in Ihrem Unternehmen überwachen und untersuchen. Um diese Funktion zu vereinfachen, AWS Security Incident Response wird automatisch eine dienstbezogene Rolle für alle betroffenen Mitgliedskonten innerhalb Ihres AWS Organizations Unternehmens erstellt. Für das Verwaltungskonto müssen Sie die dienstbezogene Rolle jedoch manuell erstellen, um die Überwachung zu aktivieren.

Der Dienst kann die dienstverknüpfte Rolle im Verwaltungskonto nicht erstellen. Sie müssen diese Rolle manuell im Verwaltungskonto erstellen, indem Sie mit AWS CloudFormation Stack-Sets arbeiten.

Grundlegendes zur automatischen Archivierung mit Proactive Response

Wenn Sie proaktive Reaktion und Alert-Triaging aktivieren, AWS Security Incident Response werden die Sicherheitsergebnisse von Amazon und Security Hub CSPM automatisch überwacht GuardDuty und bewertet. Im Rahmen dieses Auto-Triage-Workflows werden die Ergebnisse automatisch anhand der folgenden Kriterien archiviert:

Verhalten bei der automatischen Archivierung:

- Gutartige Ergebnisse: Wenn der Auto-Triage-Prozess feststellt, dass ein Ergebnis harmlos ist (keine echte Sicherheitsbedrohung), wird das Ergebnis AWS Security Incident Response automatisch in Amazon archiviert GuardDuty und Unterdrückungsregeln erstellt, um zu verhindern, dass ähnliche Ergebnisse in future Warnmeldungen auslösen.
- Unterdrückungsregeln: Der Service erstellt Unterdrückungs- und automatische Archivierungsregeln sowohl in Amazon GuardDuty als auch in Security Hub CSPM für Ergebnisse, die den zweifelsfrei funktionierenden Mustern Ihrer Umgebung entsprechen, z. B. erwartete IP-Adressen, IAM-Entitäten und normales Betriebsverhalten.
- Geringeres Alarmvolumen: Organizations, die SIEM-Technologie verwenden, verzeichnen im Laufe der Zeit ein deutlich GuardDuty geringeres Suchvolumen von Amazon, da der Service Ihre Umgebung erkennt und automatisch harmlose Ergebnisse archiviert. Dies verbessert die Effizienz sowohl für den AWS Security Incident Response Service als auch für Ihr SIEM.

Archivierte Ergebnisse anzeigen:

Sie können automatisch archivierte Ergebnisse und die Unterdrückungsregeln überprüfen, die erstellt wurden von AWS Security Incident Response:

1. Navigieren Sie zur GuardDuty Amazon-Konsole
2. Wählen Sie Findings
3. Wählen Sie im Ergebnisfilter Archiviert
4. Überprüfen Sie die Unterdrückungsregeln, indem Sie neben jeder Regel auf den Abwärtspfeil klicken

Wichtige Überlegungen:

- Archivierte Ergebnisse werden 90 Tage lang bei Amazon GuardDuty aufbewahrt und können in diesem Zeitraum jederzeit eingesehen werden.

- Sie können Unterdrückungsregeln jederzeit über die GuardDuty Amazon-Konsole ändern oder löschen
- Der Auto-Triage-Prozess passt sich kontinuierlich an Ihre Umgebung an, verbessert die Genauigkeit im Laufe der Zeit und reduziert Fehlalarme

Eindämmung: AWS Security Incident Response Kann im Falle eines Sicherheitsvorfalls Eindämmungsmaßnahmen ergreifen, um die Auswirkungen schnell zu mildern, z. B. die Isolierung kompromittierter Hosts oder die Rotation von Zugangsdaten. Security Incident Response aktiviert standardmäßig keine Eindämmungsfunktionen. Um diese Eindämmungsmaßnahmen auszuführen, müssen Sie dem Service zunächst die erforderlichen Berechtigungen erteilen. Dies kann durch die Bereitstellung von erreicht werden AWS CloudFormation StackSet, wodurch die erforderlichen Rollen erstellt werden.

Benutzeraufgaben

Inhalt

Dashboard

Auf der AWS Security Incident Response Konsole bietet Ihnen das Dashboard einen Überblick über Ihr Incident-Response-Team, Ihren proaktiven Reaktionsstatus und eine fortlaufende Anzahl von Fällen über vier Wochen.

Team für die Reaktion auf Vorfälle

Wählen Sie Incident Response Team anzeigen aus, um auf Details zu Ihren Incident-Response-Teamkollegen zuzugreifen.

Meine Fälle

Im Bereich Meine Fälle des Dashboards wird die Anzahl der geöffneten und geschlossenen AWS unterstützten Fälle sowie die Anzahl der selbst verwalteten Fälle angezeigt, die Ihnen innerhalb eines bestimmten Zeitraums zugewiesen wurden. Außerdem wird die durchschnittliche Zeit, die zur Lösung der abgeschlossenen Fälle benötigt wurde, in Stunden angezeigt.

Ich verwalte mein Incident Response Team

Ihr Incident-Response-Team besteht aus Stakeholdern für den Incident-Response-Prozess. Im Rahmen Ihrer Mitgliedschaft können Sie bis zu zehn Stakeholder konfigurieren.

Zu den internen Stakeholdern gehören beispielsweise Mitglieder Ihres Incident-Response-Teams, Sicherheitsanalysten, Anwendungseigentümer und Ihr Sicherheitsteam.

Zu den externen Stakeholdern gehören beispielsweise Personen von unabhängigen Softwareanbietern (ISV) und Managed Service Providern (MSP), die Sie in einen Incident-Response-Prozess einbeziehen möchten.

> **Note**
>
> Durch die Einrichtung Ihres Incident-Response-Teams erhalten Teammitglieder nicht automatisch Zugriff auf Serviceressourcen wie Mitgliedschaften und Fälle. Sie können AWS verwaltete Richtlinien verwenden AWS Security Incident Response , um Lese- und Schreibzugriff auf Ressourcen zu gewähren. Klicken Sie hier, um mehr zu erfahren.

Ihre auf einer Mitgliedschaftsstufe angegebenen Teammitglieder für die Reaktion auf Vorfälle werden automatisch zu jedem Fall hinzugefügt. Sie können jederzeit einzelne Teammitglieder hinzufügen oder entfernen, nachdem ein Fall erstellt wurde.

Das Incident-Response-Team erhält eine E-Mail-Benachrichtigung über die Ereignisse, die in den Kommunikationseinstellungen aufgeführt sind.

Kommunikationspräferenzen

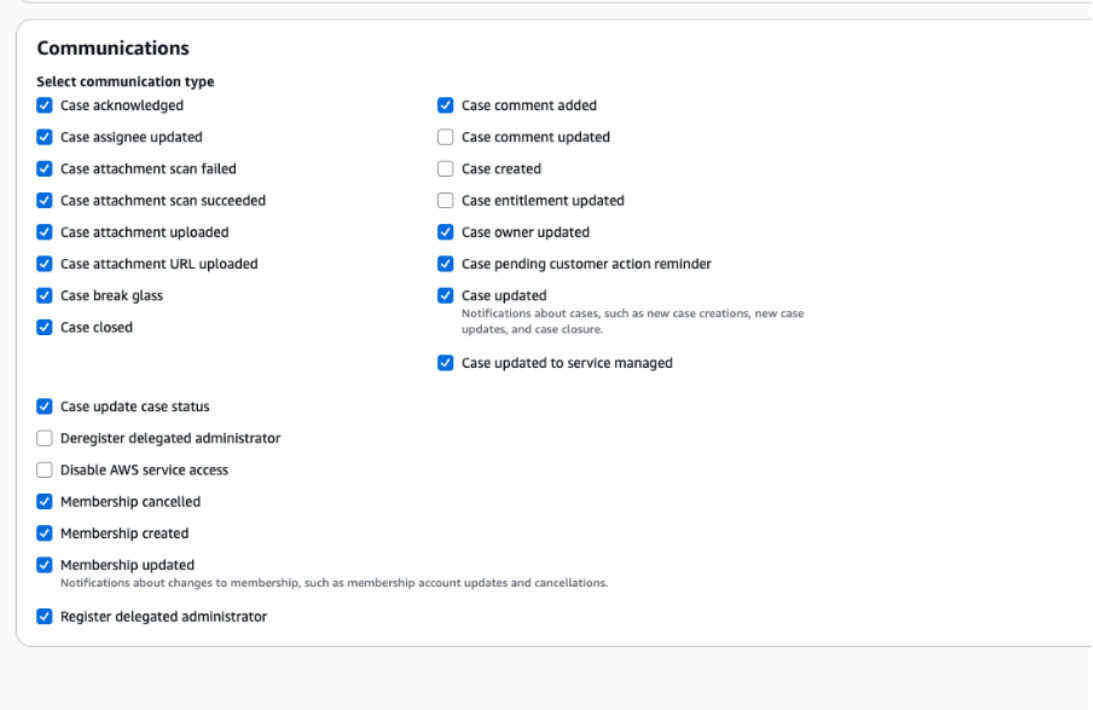
Konfigurieren Sie Ihre Kommunikationseinstellungen, um zu steuern, wie Sie bei Sicherheitsvorfällen Benachrichtigungen erhalten und mit dem Incident-Response-System interagieren.

Kommunikationseinstellungen für Ihr Team verwalten

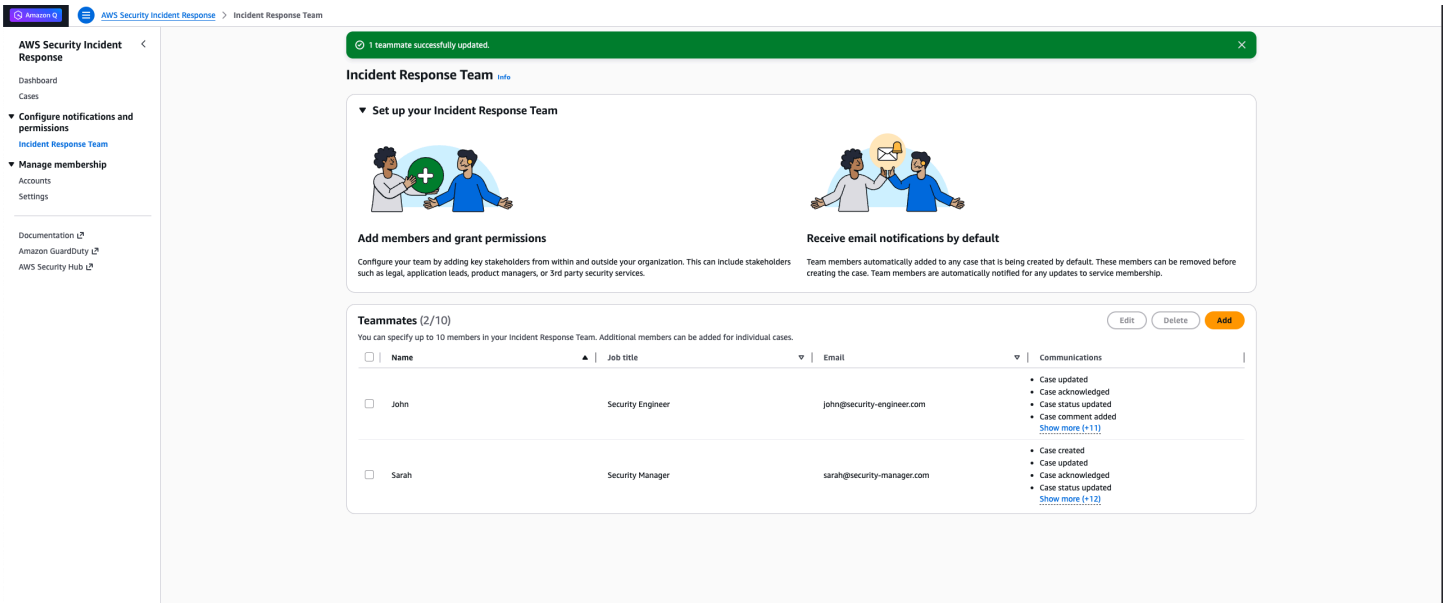
Auf der Dashboard-Seite können Sie die Kommunikationspräferenzen für einzelne Personen in Ihrem Incident-Response-Team konfigurieren.

Gehen Sie wie folgt vor, um die Kommunikationseinstellungen für Teammitglieder zu verwalten:

1. Navigieren Sie von Ihrem Dashboard aus zur Seite des Incident Response Teams
2. Führen Sie eine der folgenden Aktionen aus:
   - Um ein vorhandenes Teammitglied zu aktualisieren: Wählen Sie das Teammitglied aus, dessen Kommunikationseinstellungen Sie ändern möchten, und wählen Sie dann Bearbeiten
   - Um ein neues Teammitglied hinzuzufügen: Wähle Hinzufügen
3. Am Ende des Formulars sehen Sie Kommunikation
   a. Wählen Sie die Kontrollkästchen für Mitteilungen aus, die Sie erhalten möchten
   b. Deaktivieren Sie die Kontrollkästchen für Mitteilungen, die Sie nicht erhalten möchten



4. Speichern Sie Ihre Änderungen



Standard-Kommunikationseinstellungen

Standardmäßig ist für Mitglieder des Incident-Response-Teams die gesamte Kommunikation aktiviert. Sie können diese Einstellungen jederzeit mit den oben genannten Schritten ändern.

Kommunikationsoptionen

Ihre Kommunikationseinstellungen steuern, wie Sie mit dem Incident Response System interagieren und wie Ihnen bei Sicherheitsvorfällen Benachrichtigungen zugestellt werden.

> **Note**
>
> Diese Einstellungen gelten für die gesamte future Kommunikation innerhalb des Security Incident Response-Systems. Sie können diese Einstellungen jederzeit ändern, indem Sie die obigen Schritte wiederholen.

Kontozuweisung zu AWS Organizations

Wenn Sie die Option aktivieren AWS Security Incident Response, haben Sie die Möglichkeit, Ihre gesamte Organisation oder bestimmte Organisationseinheiten auszuwählen (OUs). Wenn bestimmte Konten ausgewählt OUs sind, deckt Ihre Mitgliedschaft nur die Konten ab, die zu den ausgewählten Konten gehören OUs. Wenn die gesamte Organisation ausgewählt ist, deckt Ihre Mitgliedschaft alle Konten innerhalb Ihrer Organisation ab.

Weitere Informationen finden Sie unter AWS Security Incident Response Konten verwalten mit AWS Organizations.

Verwaltung Ihres Mitgliedschaftsschutzes

Sie können Ihre Versicherungsoption jederzeit ändern, einschließlich der Umstellung vom unternehmensweiten Versicherungsschutz auf einen spezifischen Versicherungsschutz. OUs

Aktualisierung von OU-Zuordnungen

So verwalten Sie den Versicherungsschutz Ihrer Mitgliedschaft:

1. Navigieren Sie zur Seite mit den Einstellungen für die Kontoverknüpfung
2. Wählen Sie Hinzufügen aus OUs, um das auszuwählen, was OUs Sie mit Ihrer Mitgliedschaft verknüpfen möchten
3. Wählen OUs Sie die aus, die Sie mit Ihrer Mitgliedschaft verknüpfen möchten
4. Klicken Sie auf Zuordnung aktualisieren, um die OU-Zuordnung in Ihrer Mitgliedschaft zu speichern

Nachdem Sie Ihre Verknüpfungen aktualisiert haben, können Sie zur gleichen Seite zurückkehren und alle Verknüpfungen entfernen OUs , die Sie von Ihrer Mitgliedschaft trennen möchten. Diese Flexibilität gilt auch dann, wenn Sie zunächst Ihre gesamte Organisation ausgewählt haben. Sie können Ihre Mitgliedschaft später so aktualisieren, dass sie nur bestimmte Bereiche abdeckt, OUs ohne den Service kündigen und erneut aktivieren zu müssen.

Weitere Informationen finden Sie unter Mitgliedschaft mit Organisationseinheiten verwalten (). OUs

Wichtige Überlegungen

Konten direkt unter dem Stammverzeichnis: Wenn Sie bestimmte Konten OUs für Ihre Mitgliedschaft auswählen, werden Konten, die sich direkt unter dem Stammverzeichnis der Organisation befinden (nicht Teil einer Organisationseinheit), nicht mit Ihrer Mitgliedschaft verknüpft. Um diese Konten in den Geltungsbereich Ihrer Mitgliedschaft aufzunehmen, müssen Sie sie zunächst einer Organisationseinheit hinzufügen und diese dann Ihrer Mitgliedschaft zuordnen.

> **Note**
>
> Wir verbessern kontinuierlich die Benutzererfahrung der OU Association, um den Vorgang intuitiver und selbsterklärender zu gestalten.

Überwachung und Untersuchung

AWS Security Incident Response überprüft und sortiert Sicherheitswarnungen von Amazon GuardDuty und konfiguriert dann Unterdrückungsregeln auf der Grundlage Ihrer Umgebung AWS Security Hub CSPM, um unnötige Warnungen zu verhindern. Das AWS Security Incident Response Engineering-Team (SIRE) untersucht die Ergebnisse und eskaliert und leitet Ihr Team schnell an, um potenzielle Probleme schnell einzudämmen. Falls gewünscht, können Sie die AWS Security Incident Response Genehmigung zur Durchführung von Eindämmungsmaßnahmen in Ihrem Namen erteilen.

AWS Security Incident Response entspricht dem NIST 800-61r2 Computer Security Event Handling Guide for Security Event Response. Die Ausrichtung an diesem Industriestandard AWS Security Incident Response bietet einen konsistenten Ansatz für das Management von Sicherheitsereignissen und die Einhaltung bewährter Verfahren bei der Absicherung und Reaktion auf Sicherheitsereignisse in Ihrer Umgebung. AWS

Wenn eine AWS Security Incident Response Sicherheitswarnung erkannt wird oder Sie Sicherheitsunterstützung anfordern, untersucht das AWS SIRE das Problem. Das Team sammelt

Protokollereignisse und Servicedaten wie GuardDuty Warnmeldungen, sortiert und analysiert diese Daten, führt Maßnahmen zur Behebung und Eindämmung durch und erstellt Berichte nach dem Vorfall.

Inhalt

Vorbereitung

Das AWS Security Incident Response Team untersucht und arbeitet während des gesamten Lebenszyklus der Reaktion auf Sicherheitsereignisse mit Ihnen zusammen. Es wird empfohlen, dieses Team zusammenzustellen und die erforderlichen Berechtigungen zuzuweisen, bevor ein Sicherheitsereignis eintritt.

Erkennen und Analysieren

Ein Ereignis melden

Sie können über das AWS Security Incident Response Portal ein Sicherheitsereignis auslösen. Es ist wichtig, während eines Sicherheitsereignisses nicht zu warten. AWS Security Incident Response verwendet automatisierte und manuelle Techniken, um Sicherheitsereignisse zu untersuchen, Protokolle zu analysieren und nach anomalen Mustern zu suchen. Ihre Partnerschaft und Ihr Verständnis Ihrer Umgebung beschleunigen diese Analyse.

Aktivierung unterstützter Erkennungsquellen

> **Note**
>
> AWS Security Incident Response Die Servicekosten beinhalten keine Nutzungs- und sonstigen Kosten und Gebühren im Zusammenhang mit unterstützten Erkennungsquellen

oder der Nutzung anderer AWS Dienste. Einzelheiten zu den Kosten finden Sie auf den Seiten der einzelnen Funktionen oder Dienste.

Amazon GuardDuty

Informationen zur Aktivierung GuardDuty in Ihrer gesamten Organisation finden Sie im `Setting up GuardDuty` Abschnitt des GuardDuty Amazon-Benutzerhandbuchs.

Wir empfehlen Ihnen dringend, alle unterstützten GuardDuty Optionen zu aktivieren AWS-Regionen. Auf diese Weise können GuardDuty Sie auch in Regionen, die Sie nicht aktiv nutzen, Erkenntnisse über unbefugte oder ungewöhnliche Aktivitäten gewinnen. Weitere Informationen finden Sie unter GuardDuty Amazon-Regionen und -Endpunkte

GuardDuty Die Aktivierung ermöglicht AWS Security Incident Response den Zugriff auf wichtige Daten zur Bedrohungserkennung und verbessert so die Fähigkeit, potenzielle Sicherheitsprobleme in Ihrer AWS Umgebung zu erkennen und darauf zu reagieren.

AWS Security Hub CSPM

Security Hub CSPM kann Sicherheitsergebnisse von verschiedenen AWS Diensten und unterstützten Sicherheitslösungen von Drittanbietern aufnehmen. Diese Integrationen können dabei helfen, Ergebnisse anderer Erkennungstools zu AWS Security Incident Response überwachen und zu untersuchen.

Informationen zur Aktivierung von Security Hub CSPM mit Organisationsintegration finden Sie im AWS Security Hub CSPM Benutzerhandbuch.

Es gibt mehrere Möglichkeiten, Integrationen auf Security Hub CSPM zu aktivieren. Für Integrationen von Drittanbieterprodukten müssen Sie die Integration möglicherweise bei der erwerben und AWS Marketplace anschließend konfigurieren. Die Integrationsinformationen enthalten Links, mit denen Sie diese Aufgaben ausführen können. Erfahren Sie mehr darüber, wie Sie AWS Security Hub CSPM Integrationen aktivieren können.

AWS Security Incident Response kann die Ergebnisse der folgenden Tools überwachen und untersuchen, wenn diese integriert AWS Security Hub CSPM sind:

- CrowdStrike — CrowdStrike Falke
- Schnürarbeiten — Schnürarbeiten
- Trend Micro — Cloud Eins

Durch die Aktivierung dieser Integrationen können Sie den Umfang und die Effektivität der Überwachungs- und AWS Security Incident Response Ermittlungsfunktionen erheblich verbessern.

Erkennung

Wenn „Proactive Response“ aktiviert ist, https://docs.aws.amazon.com/security-ir/latest/userguide/setup AWS Security Incident Response nimmt monitoring-and-investigation-workflows .html Ergebnisse von Amazon GuardDuty und AWS Security Hub CSPM anhand von EventBridge Amazon-Regeln auf, die während des Onboardings auf Ihre Konten übertragen werden.

AWS Security Incident Response archiviert automatisch GuardDuty Amazon-Ergebnisse, die während der automatisierten Triage als harmlos eingestuft wurden oder mit erwarteten Aktivitäten in Verbindung stehen. Sie können archivierte Ergebnisse in der GuardDuty Amazon-Konsole anzeigen, indem Sie im Filter Status der Ergebnisse die Option Archiviert auswählen. Weitere Informationen finden Sie im GuardDuty Amazon-Benutzerhandbuch unter Generierte Ergebnisse in der GuardDuty Konsole anzeigen.

AWS Security Incident Response archiviert automatisch GuardDuty Amazon-Ergebnisse, die während der automatisierten Triage als harmlos eingestuft wurden oder mit erwarteten Aktivitäten in Verbindung stehen. Diese Archivierung erfolgt nur für Ergebnisse, die einer Triage unterzogen wurden und deren Ergebnis als „Archiv“ bezeichnet wurde. Ergebnisse, die derzeit untersucht werden, bleiben auch nach Abschluss einer Untersuchung in der GuardDuty Amazon-Konsole sichtbar. Sie können archivierte Ergebnisse in der GuardDuty Amazon-Konsole anzeigen, indem Sie im Ergebnisfilter Archiviert auswählen. Weitere Informationen zur Arbeit mit archivierten Ergebnissen finden Sie unter Arbeiten mit Ergebnissen im GuardDuty Amazon-Benutzerhandbuch.

Bei AWS Security Hub CSPM der Erfassung von Sicherheitsergebnissen aktualisiert das System jedes Ergebnis mit einem Hinweis, dass die automatische Prüfung begonnen hat. Der Workflow-Status ändert sich von NEU in BENACHRICHTIGT, wodurch das Ergebnis aus der Standardansicht der AWS Security Hub CSPM Ergebnisse entfernt wird. Wenn die Triage feststellt, dass ein Ergebnis harmlos ist oder mit einer erwarteten Aktivität zusammenhängt, fügt das System dem Ergebnis eine Notiz hinzu und aktualisiert den Workflow-Status auf UNTERDRÜCKT.

Analyse: Automatisierte Triage

AWS Security Incident Response analysiert automatisch Sicherheitsresultate. Der Triage-Prozess bestimmt, ob die erkannte Aktivität dem erwarteten Verhalten entspricht, indem Daten aus mehreren Quellen analysiert werden, darunter die gefundene Nutzlast, AWS Dienstmetadaten, AWS Protokollierungs- und Überwachungsdaten (wie AWS CloudTrail VPC-Flow-Logs), AWS

Bedrohungsinformationen und den Kontext, den Sie über Ihre AWS und Ihre lokalen Umgebungen bereitstellen können.

Wenn die automatische Triage feststellt, dass die erkannte Aktivität erwartet wird, ergreift das System keine weiteren Ermittlungsmaßnahmen.

Analyse: Reaktion auf Sicherheitsvorfälle

AWS Security Incident Response Engineering ist ein globales, stets verfügbares Team von Sicherheitsexperten mit Fachwissen in der Reaktion auf Sicherheitsvorfälle AWS und der Reaktion auf Sicherheitsvorfälle. Wenn durch die automatische Triage nicht festgestellt werden kann, dass die Aktivität erwartet wird, wird die AWS Security Incident Response technische Abteilung mit der Durchführung einer Sicherheitsuntersuchung beauftragt. Wenn das Ereignis von Security Hub aufgenommen wurde, wird ein Hinweis zu dem entsprechenden Ergebnis veröffentlicht, der besagt, dass die Untersuchung durch AWS Security Incident Response Engineering im Gange ist.

AWS Security Incident Response Engineering führt eine praktische Sicherheitsuntersuchung durch, indem es zusätzliche Servicemetadaten und Bedrohungsinformationen analysiert, Erkenntnisse aus früheren Erkenntnissen und Untersuchungen in Ihrer Umgebung überprüft und Fachwissen zur Reaktion auf Vorfälle einsetzt. Abhängig von Ihren Containment-Einstellungen (siehe Contain) kann AWS Security Incident Response Engineering das Incident Response Team Ihres Unternehmens anhand eines Security Incident Response-Falls in der AWS Security Incident Response Konsole kontaktieren, um zu überprüfen, ob die erkannte Aktivität erwartet und autorisiert ist. Reaktion auf einen AWS generierten Fall.

Kommunizieren

AWS Security Incident Response hält Sie bei Sicherheitsuntersuchungen auf dem Laufenden, indem es Ihr Incident Response-Team im Rahmen eines Security Incident Response-Falls kontaktiert. Eine Untersuchung kann von mehreren AWS Security Incident Response Technikern unterstützt werden. Die Kommunikation kann Folgendes umfassen: Bestätigung oder Benachrichtigung über die Einleitung einer Sicherheitsuntersuchung, Einrichtung einer Call Bridge, Analyse von Artefakten wie Protokolldateien, Anfragen zur Bestätigung erwarteter Aktivitäten und Weitergabe von Untersuchungsergebnissen.

Wenn Sie Ihr Incident-Response-Team AWS Security Incident Response proaktiv einbeziehen, wird ein Fall in Ihrem AWS Security Incident Response Mitgliedskonto erstellt, wodurch die Kommunikation für alle Unternehmenskonten an einem Ort zentralisiert wird. Diese Fälle enthalten das Präfix „[Proactive case]“ im Titel, wodurch sie als initiiert von identifiziert werden. AWS Security Incident Response Indem Ihr Incident-Response-Team aktiv auf diese Mitteilungen eingeht und

zeitnah darauf reagiert, kann es Sie bei folgenden Aufgaben unterstützen AWS Security Incident Response :

- Sorgen Sie für eine schnelle Reaktion auf echte Sicherheitsvorfälle.
- Machen Sie sich mit Ihrer Umgebung und den erwarteten Verhaltensweisen vertraut.
- Reduzieren Sie im Laufe der Zeit die Anzahl falsch positiver Erkennungen.

Die Effektivität von AWS Security Incident Response verbessert sich mit Ihrer Zusammenarbeit und führt zu einer besser überwachten und sichereren AWS Umgebung.

Aktualisierung der Ergebnisse

AWS Security Incident Response verwaltet Ergebnisse je nach Quelle und Ergebnis der Triage unterschiedlich.

Optimierung der Dienste

Wenn Ihre Kontoservice-Kontingente dies zulassen, wird AWS Security Incident Response versucht, eine GuardDuty Amazon-Unterdrückungsregel oder eine AWS Security Hub CSPM Automatisierungsregel bereitzustellen. Diese Regeln unterdrücken future Ergebnisse, die dem Typ und der Quelle bekannter autorisierter Aktivitäten entsprechen (z. B. Quell-IP-Adresse, ASN, Identity Principal oder Ressource). AWS Security Hub CSPM Regeln werden mit Priorität 10 bereitgestellt, sodass Sie diese Automatisierungen bei Bedarf mit selbst definierten Regeln außer Kraft setzen können.

Auf diese Weise stimmen Sie die AWS Security Incident Response Erkennungsquellen auf der Grundlage des erwarteten Verhaltens in Ihrer AWS Umgebung ab. Ihr Incident Response Team wird über Änderungen an diesen Regelsätzen informiert, und Änderungen werden auf Anfrage rückgängig gemacht.

KI-Ermittlungsagent

-Übersicht

Der KI-gestützte Ermittlungsagent arbeitet mit Kunden und AWS Security Incident Response Ingenieuren zusammen, um Sicherheitsuntersuchungen zu beschleunigen. Wenn ein Kunde einen AWS unterstützten Fall erstellt, wird der Agent automatisch parallel zum Einsatz des Security Incident Response-Technikers aktiviert, wodurch die Lösungszeit von Tagen auf Stunden reduziert wird.

Bei Kundeneskalationen können Fälle zur Reaktion auf Sicherheitsvorfälle von Ihnen oder proaktiv von Ihnen erstellt werden. AWS Security Incident Response Wenn ein neuer AWS unterstützter

Fall erstellt wird, wird der Investigative Agent automatisch ausgelöst. Sie können alle Fälle über die Konsole, API oder EventBridge Amazon-Integrationen verwalten.

Die wichtigsten Vorteile

- Parallele Untersuchung — Der Agent arbeitet gleichzeitig mit den Einsatzkräften zusammen und bietet sowohl KI-gestützte Automatisierung als auch menschliches Fachwissen.
- Automatisierte Beweiserhebung — Eliminiert die manuelle Protokollanalyse durch automatische Abfragen AWS CloudTrail, IAM, Amazon EC2 und Cost Explorer.
- Benutzeroberfläche in natürlicher Sprache — Beschreiben Sie Sicherheitsbedenken in einfacher Sprache, ohne dass Sie sich mit Protokollformaten auskennen müssen. AWS
- Schnellere Reaktion — Zusammenfassungen der Ermittlungen sind innerhalb weniger Minuten auf der Registerkarte Untersuchung verfügbar.
- Vollständige Überprüfbarkeit — Alle Agentenaktionen werden AWS CloudTrail unter der `AWSServiceRoleForSupport` Rolle protokolliert.

> **Important**
>
> Diese Funktion ist nur für Fälle verfügbar, die von AWS-unterstützt werden. Selbstverwaltete Fälle beinhalten keine KI-Ermittlungsfunktionen.

Funktionsweise

Der KI-Ermittlungsagent folgt bei der Analyse AWS unterstützter Sicherheitsfälle einem strukturierten Arbeitsablauf:

Arbeitsablauf bei der Untersuchung

1. Fallerstellung — Der Kunde erstellt in der Security Incident Response-Konsole einen AWS unterstützten Fall, in dem das Sicherheitsproblem beschrieben wird.
2. Parallele Aktivierung
   - Die Techniker für die Reaktion auf Sicherheitsvorfälle befassen sich mit dem Fall.
   - Gleichzeitig beginnt der KI-Agent mit seinem Ermittlungsablauf.
3. Kontextfragen (optional) — Der Agent kann klärende Fragen stellen, um spezifische Informationen zu erhalten:

- AWS Betroffenes Konto IDs
- Beteiligte IAM-Prinzipale (Benutzer, Rollen, Zugriffsschlüssel)
- Spezifische Ressourcen-Identifikatoren (S3-Buckets, EC2-Instances,) ARNs
- Zeitrahmen verdächtiger Aktivitäten

4. Erfassung von Beweisen — Der Agent fragt automatisch AWS Datenquellen ab:
   - AWS CloudTrail— API-Aufrufe und Aktivitäten im Zusammenhang mit dem Vorfall
   - IAM — Benutzer- und Rollenberechtigungen, Richtlinienänderungen und Erstellung neuer Identitäten
   - Amazon EC2 EC2-Instance APIs — Informationen zu Rechenressourcen, falls betroffen
   - Cost Explorer — Kosten- und Nutzungskennzahlen für ungewöhnlichen Ressourcenverbrauch
5. Analyse und Korrelation — Der Agent korreliert Beweise für verschiedene Dienste, identifiziert Muster und erstellt einen Zeitplan für Ereignisse.
6. Generierung von Zusammenfassungen — Innerhalb weniger Minuten präsentiert der Agent auf der Registerkarte Untersuchung eine umfassende Zusammenfassung der Untersuchung.

> **Note**
>
> Alle Felder sind optional. Wenn innerhalb von 10 Minuten keine Antwort erfolgt, wird die Untersuchung automatisch gestartet. In einigen Fällen, wenn bereits ausreichende Informationen verfügbar sind, kann der Mitarbeiter die optionalen Fragen vollständig überspringen.

Zugriff auf Untersuchungsergebnisse

So sehen Sie sich die KI-Analyse an:

1. Navigieren Sie in der Security Incident Response-Konsole zu Ihrem Fall.
2. Wählen Sie den Tab Investigation aus.
3. Sehen Sie sich die Zusammenfassung der Untersuchung mit Ergebnissen, Zeitplan und Kontext an.

Die Zusammenfassung der KI-Ermittlungsbeamten wird automatisch als Kommentar im Bereich Kommunikation des Falls veröffentlicht, sodass sie zusammen mit anderen Fallaktualisierungen leicht überprüft werden kann.

Datenzugriff und Berechtigungen

Der KI-Ermittlungsagent verwendet die `AWSServiceRoleForSupport` serviceverknüpfte Rolle, um auf AWS Ressourcen zuzugreifen. Diese Rolle bietet nur Leseberechtigungen, die für die Beweiserhebung erforderlich sind.

Alle vom Agenten ausgeführten Aktionen werden angemeldet AWS CloudTrail, sodass Kunden genau überprüfen können, auf welche Daten während der Untersuchung zugegriffen wurde. In den AWS CloudTrail Protokollen werden diese Aktionen zugeordnet`AWSServiceRoleForSupport`.

Voraussetzungen

Bevor Sie die KI-gestützten Ermittlungsfunktionen nutzen, stellen Sie Folgendes sicher:

Erforderliches Setup

- AWS Security Incident Response aktiviert — Der Dienst muss über das AWS Organizations Verwaltungskonto aktiviert werden.
- AWS unterstützter Falltyp — Die KI-Untersuchung ist nur für AWS unterstützte Fälle (nicht für selbst verwaltete Fälle) verfügbar.
- AWSServiceRoleForSupport— Diese dienstbezogene Rolle wird automatisch erstellt und gewährt dem Ermittler die erforderlichen Berechtigungen.

Erforderliche -Berechtigungen

Um AWS unterstützte Fälle zu erstellen und auf Untersuchungsergebnisse zuzugreifen, benötigt der IAM-Principal die folgenden Berechtigungen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "security-ir:CreateCase",
                "security-ir:GetCase",
                "security-ir:ListCases",
                "security-ir:UpdateCase"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Den Ermittlungsagenten verwenden

Der KI-Ermittlungsagent wird automatisch aktiviert, wenn ein Fall erstellt wird, der von der KI AWS unterstützt wird.

Um den Fortschritt der KI-Untersuchung zu überwachen

1. Öffnen Sie Ihren Fall in der AWS Security Incident Response Konsole.
2. Wählen Sie den Tab Untersuchung.
3. Zeigen Sie den Status der Untersuchung an (In Bearbeitung oder Abgeschlossen).
4. Lesen Sie nach Abschluss die umfassende Zusammenfassung der Untersuchung mit Ergebnissen, Zeitplan und Empfehlungen.

Verantwortungsvolle Offenlegung von KI

Zusammenfassungen von Untersuchungen werden mithilfe AWS generativer KI-Funktionen erstellt. Sie sind dafür verantwortlich, KI-generierte Empfehlungen in Ihrem spezifischen Kontext zu bewerten, geeignete Aufsichtsmechanismen zu implementieren, die Ergebnisse unabhängig zu verifizieren und die menschliche Aufsicht über alle Sicherheitsentscheidungen aufrechtzuerhalten.

Verwendung von Kundendaten

AI Investigative Agent verwendet keine Kundendaten für Modelltrainings und gibt Kundendaten nicht an Dritte weiter.

Enthalten

AWS Security Incident Response arbeitet mit Ihnen zusammen, um Ereignisse einzudämmen. Sie können den Service so konfigurieren, dass er als Reaktion auf Sicherheitslücken proaktive Eindämmungsmaßnahmen in Ihrem Konto ergreift. Sie können die Eindämmung auch selbst oder in Partnerschaft mit Ihren Partnern durchführen, indem Sie die unter Unterstützte Sicherheitsmaßnahmen beschriebenen SSM-Dokumente verwenden.

> **Important**
>
> AWS Security Incident Response aktiviert standardmäßig keine Containment-Funktionen.

Zwei Schritte sind erforderlich, um proaktive Eindämmungsfunktionen zu aktivieren:

1. Erteilen Sie dem Service mithilfe von IAM-Rollen die erforderlichen Berechtigungen. Sie können diese Rollen einzeln pro Konto oder für Ihre gesamte Organisation erstellen, indem Sie mit AWS CloudFormation Stacksets arbeiten, die die erforderlichen Rollen erstellen.
2. Definieren Sie Ihre Containment-Einstellungen pro Konto oder unternehmensweit, um proaktive Eindämmungsmaßnahmen zu autorisieren. Einstellungen auf Kontoebene haben Vorrang vor Einstellungen auf Organisationsebene. Dies kann durch die Erstellung eines AWS Support-Falls (technisch: Security Incident Response Service/Other) geschehen. Die verfügbaren Containment-Einstellungen sind:
   - Genehmigung erforderlich (Standard): Führen Sie keine proaktive Eingrenzung von Ressourcen ohne ausdrückliche Genehmigung auf einer case-by-case bestimmten Grundlage durch.
   - Bestätigt eindämmen: Führt eine proaktive Eingrenzung einer Ressource durch, bei der bestätigt wurde, dass sie gefährdet ist.
   - Vermuteten Schaden eindämmen: Führen Sie eine proaktive Eingrenzung einer Ressource durch, bei der die Wahrscheinlichkeit hoch ist, dass sie gefährdet wurde, und zwar auf der Grundlage einer Analyse durch AWS Security Incident Response Engineering.

Entscheidungsfindung bei der Eindämmung

Ein wesentlicher Bestandteil der Eindämmung ist die Entscheidungsfindung, z. B. ob ein System heruntergefahren, eine Ressource vom Netzwerk isoliert, der Zugriff deaktiviert oder Sitzungen beendet werden sollen. Diese Entscheidungen werden einfacher, wenn es vorher festgelegte Strategien und Verfahren gibt, um das Ereignis einzudämmen. AWS Security Incident Response liefert die Eindämmungsstrategie, informiert Sie über mögliche Auswirkungen und unterstützt Sie bei der Implementierung der Lösung erst, nachdem Sie die damit verbundenen Risiken abgewogen und ihnen zugestimmt haben.

Unterstützte Eindämmungsmaßnahmen

AWS Security Incident Response führt in Ihrem Namen unterstützte Eindämmungsmaßnahmen aus, um die Reaktion zu beschleunigen und die Zeit zu verkürzen, die ein Bedrohungsakteur benötigt, um in Ihrer Umgebung potenziell Schaden anzurichten. Diese Funktion ermöglicht eine schnellere Abwehr identifizierter Bedrohungen, minimiert potenzielle Auswirkungen und verbessert Ihre allgemeine Sicherheitslage. Je nach den zu analysierenden Ressourcen gibt es unterschiedliche

Eindämmungsoptionen. Die unterstützten Eindämmungsmaßnahmen werden in den folgenden Unterabschnitten beschrieben.

EC2-Eindämmung

Die `AWSSupport-ContainEC2Instance` Containment-Automatisierung führt eine umkehrbare Netzwerkeindämmung einer EC2-Instance durch, wobei die Instance intakt bleibt und läuft, sie jedoch von jeder neuen Netzwerkaktivität isoliert wird und verhindert, dass sie mit Ressourcen innerhalb und außerhalb Ihrer VPC kommuniziert.

> **Important**
>
> Es ist wichtig zu beachten, dass bestehende nachverfolgte Verbindungen nicht aufgrund von wechselnden Sicherheitsgruppen geschlossen werden — nur future Datenverkehr wird durch die neue Sicherheitsgruppe und dieses SSM-Dokument effektiv blockiert. Weitere Informationen finden Sie im Abschnitt Source Containment des technischen Leitfadens zum Service.

IAM-Eindämmung

Die `AWSSupport-ContainIAMPrincipal` Containment-Automatisierung führt eine umkehrbare Netzwerkeindämmung eines IAM-Benutzers oder einer IAM-Rolle durch, sodass der Benutzer oder die Rolle in IAM verbleibt, sie jedoch von der Kommunikation mit Ressourcen in Ihrem Konto isoliert wird.

S3-Eindämmung

Die `AWSSupport-ContainS3Resource` Containment-Automatisierung führt eine umkehrbare Beschränkung eines S3-Buckets durch, wobei die Objekte im Bucket belassen und der Amazon S3-Bucket oder das Amazon S3-Objekt durch Änderung seiner Zugriffsrichtlinien isoliert werden.

Entwicklung von Eindämmungsstrategien

AWS Security Incident Response ermutigt Sie, für jede Art von Großereignis Eindämmungsstrategien in Betracht zu ziehen, die Ihrer Risikobereitschaft entsprechen. Dokumentieren Sie klare Kriterien, um Ihnen bei der Entscheidungsfindung während einer Veranstaltung zu helfen. Zu den zu berücksichtigenden Kriterien gehören:

- Mögliche Schäden an Ressourcen

- Beweissicherung und regulatorische Anforderungen
- Nichtverfügbarkeit von Diensten (z. B. Netzwerkkonnektivität, Dienste, die für externe Parteien bereitgestellt werden)
- Zeit und Ressourcen, die für die Umsetzung der Strategie benötigt wurden
- Wirksamkeit der Strategie (z. B. teilweise oder vollständige Eindämmung)
- Dauerhaftigkeit der Lösung (z. B. reversibel oder irreversibel)
- Dauer der Lösung (z. B. Notfall-Problemumgehung, vorübergehende Behelfslösung, permanente Lösung)

Wenden Sie Sicherheitskontrollen an, die das Risiko verringern und Zeit für die Definition und Umsetzung einer effektiveren Eindämmungsstrategie bieten.

Stufenweiser Eindämmungsansatz

AWS Security Incident Response empfiehlt einen schrittweisen Ansatz zur Erreichung einer effizienten und wirksamen Eindämmung, der je nach Ressourcentyp kurz- und langfristige Strategien umfasst.

Strategie zur Eindämmung

Kann der Umfang des Sicherheitsereignisses AWS Security Incident Response ermittelt werden?

- Falls ja, identifizieren Sie alle Ressourcen (Benutzer, Systeme, Ressourcen).
- Falls nein, untersuchen Sie dies parallel zur Ausführung des nächsten Schritts für identifizierte Ressourcen.

Kann die Ressource isoliert werden?

- Falls ja, fahren Sie mit der Isolierung der betroffenen Ressourcen fort.
- Falls nein, arbeiten Sie mit den Systembesitzern und Managern zusammen, um weitere Maßnahmen zur Eindämmung des Problems zu ergreifen.

Sind alle betroffenen Ressourcen von den nicht betroffenen Ressourcen isoliert?

- Falls ja, fahren Sie mit dem nächsten Schritt fort.
- Falls nein, sollten Sie die betroffenen Ressourcen weiter isolieren, um eine kurzfristige Eindämmung zu erreichen und eine weitere Eskalation des Ereignisses zu verhindern.

Systemsicherung

Wurden für weitere Analysen Sicherungskopien der betroffenen Systeme erstellt?

Werden die forensischen Kopien verschlüsselt und an einem sicheren Ort gespeichert?

- Falls ja, fahren Sie mit dem nächsten Schritt fort.
- Falls nein, verschlüsseln Sie die forensischen Bilder und speichern Sie sie an einem sicheren Ort, um eine versehentliche Verwendung, Beschädigung und Manipulation zu verhindern.

Geben Sie Ihre Containment-Einstellungen ein

Um die Containment-Einstellungen für Ihr Konto oder Ihre Organisation zu konfigurieren, erstellen Sie einen AWS Support Fall.

Geben Sie in Ihrem Support-Fall die folgenden Informationen an:

Wenn konfiguriert, AWS Security Incident Response führt Executes die autorisierten Eindämmungsaktionen bei aktiven Sicherheitsvorfällen aus, um Ihre Umgebung zu schützen.

- Ihre AWS Organizations ID oder ein bestimmtes Konto IDs , für das Eindämmungsmaßnahmen autorisiert werden sollten.
- Ihre bevorzugte Eindämmungsoption.

> **Note**
>
> AWS Security Incident Response führt Containment-Aktionen nur aus, wenn sie mit den entsprechenden Einstellungen konfiguriert wurden und nachdem die erforderlichen Berechtigungen bereitgestellt wurden, um die erforderlichen Berechtigungen zu AWS CloudFormation StackSet gewähren.

Ausrotten

Während der Eliminierungsphase ist es wichtig, alle betroffenen Konten, Ressourcen und Instanzen zu identifizieren und zu beheben — beispielsweise durch das Löschen von Malware, das Entfernen kompromittierter Benutzerkonten und die Beseitigung aller entdeckten Sicherheitslücken —, um eine einheitliche Problembehebung in der gesamten Umgebung durchzuführen.

Es hat sich bewährt, bei der Beseitigung und Wiederherstellung einen schrittweisen Ansatz zu verwenden und die Maßnahmen zur Behebung nach Prioritäten zu ordnen. Der Zweck der frühen Phasen besteht darin, die allgemeine Sicherheit schnell (Tage bis Wochen) zu erhöhen und wichtige Änderungen vorzunehmen, um future Ereignisse zu verhindern. Die späteren Phasen können sich auf längerfristige Änderungen (z. B. Änderungen der Infrastruktur) und laufende Arbeiten konzentrieren, um das Unternehmen so sicher wie möglich zu halten. Jeder Fall ist einzigartig und die AWS Security Incident Response-Techniker werden mit Ihnen zusammenarbeiten, um die erforderlichen Maßnahmen zu bewerten.

Berücksichtigen Sie dabei Folgendes:

- Können Sie das System neu abbilden und es mit Patches oder anderen Gegenmaßnahmen absichern, um das Risiko von Angriffen zu verhindern oder zu verringern?
- Können Sie das infizierte System durch eine neue Instanz oder Ressource ersetzen und so eine saubere Baseline aktivieren und gleichzeitig das infizierte Objekt beenden?
- Haben Sie alle Schadsoftware und andere Artefakte entfernt, die bei der unbefugten Nutzung zurückgeblieben sind, und die betroffenen Systeme gegen weitere Angriffe abgesichert?
- Ist für die betroffenen Ressourcen eine forensische Untersuchung erforderlich?

Wiederherstellung

AWS Security Incident Response bietet Ihnen Anleitungen zur Wiederherstellung des normalen Betriebs von Systemen, zur Bestätigung, dass sie ordnungsgemäß funktionieren, und zur Behebung von Sicherheitslücken, um ähnliche Ereignisse in future zu verhindern. AWS Security Incident Response hilft nicht direkt bei der Wiederherstellung von Systemen. Zu den wichtigsten Überlegungen gehören:

- Wurden die betroffenen Systeme gepatcht und sind sie gegen den jüngsten Angriff abgesichert?
- Was ist der realisierbare Zeitplan, um die Systeme wieder in Betrieb zu nehmen?
- Welche Tools werden Sie verwenden, um die wiederhergestellten Systeme zu testen, zu überwachen und zu verifizieren?

Bericht nach dem Vorfall

AWS Security Incident Response bietet eine Zusammenfassung des Ereignisses nach Abschluss der Sicherheitsaktivitäten zwischen Ihrem und unserem Team.

Am Ende eines jeden Monats sendet der AWS Security Incident Response Service monatliche Berichte per E-Mail an den Hauptansprechpartner für jeden Kunden. Die Berichte werden im PDF-Format unter Verwendung der unten beschriebenen Kennzahlen bereitgestellt. Kunden erhalten einen Bericht pro AWS Organizations.

Fallmetriken

- Erstellte Fälle
  - Name der Dimension: Typ
  - Dimensionswerte: AWS unterstützt, selbst unterstützt
  - Einheit: Anzahl
  - Beschreibung: Die Anzahl der erstellten Fälle.
- Geschlossene Fälle
  - Name der Dimension: Typ
  - Dimensionswerte: AWS unterstützt, selbst verwaltet
  - Einheit: Anzahl
  - Beschreibung: Ein Maß für die Gesamtzahl der abgeschlossenen Fälle.
- Eröffnete Fälle
  - Name der Dimension: Typ
  - Dimensionswerte: AWS unterstützt, selbst unterstützt
  - Einheit: Anzahl
  - Beschreibung: Die Anzahl der offenen Fälle.

Triaging-Metriken

- Eingegangene Ergebnisse
  - Einheit: Anzahl
  - Beschreibung: Die Anzahl der Ergebnisse, die zur Prüfung gesendet wurden.
- Archivierte Ergebnisse
  - Einheit: Anzahl
  - Beschreibung: Die Anzahl der Ergebnisse, die nach der Verarbeitung ohne manuelle Untersuchung archiviert wurden.
- Manuell untersuchte Ergebnisse

  - Einheit: Anzahl
  - Beschreibung: Die Anzahl der Ergebnisse, bei denen eine manuelle Untersuchung durchgeführt wurde.
- Archivierte Untersuchungen
  - Einheit: Anzahl
  - Beschreibung: Die Anzahl der manuellen Untersuchungen, die zu Fehlalarmen geführt und zur Archivierung gesendet wurden
- Die Ermittlungen eskalierten
  - Einheit: Anzahl
  - Beschreibung: Die Anzahl der manuellen Untersuchungen, die zu einem Sicherheitsvorfall geführt haben

Fälle

AWS Security Incident Response ermöglicht es Ihnen, zwei Arten von Fällen zu erstellen: AWS unterstützte oder selbst verwaltete Fälle.

Erstellen Sie einen AWS unterstützten Fall

Sie können einen AWS unterstützten Fall für AWS Security Incident Response über die Konsole, die API oder die erstellen AWS Command Line Interface. AWS Unterstützte Fälle ermöglichen es Ihnen, Support von Security Incident Response-Technikern zu erhalten.

> **Important**
>
> Demo-/Simulationsfälle werden nach einem Zeitraum von 90 Tagen geschlossen.

> **Note**
>
> AWS Die Techniker für die Reaktion auf Sicherheitsvorfälle werden innerhalb von 15 Minuten auf Ihren Fall antworten. Die Reaktionszeit bezieht sich auf eine erste Antwort von Technikern für die Reaktion auf AWS Sicherheitsvorfälle. Wir werden alle zumutbaren Anstrengungen unternehmen, um Ihre erste Anfrage innerhalb dieses Zeitraums zu beantworten. Diese Antwortzeit gilt nicht für nachfolgende Antworten.

> **Note**
>
> Sie können AWS unterstützte Fälle nicht nur für aktive Sicherheitsvorfälle und Untersuchungen erstellen, sondern auch für Anfragen zu den Funktionen zur Reaktion auf AWS Sicherheitsvorfälle. Dazu gehören Fragen zu GuardDuty Unterdrückungsregeln, Konfigurationen für die Alert-Triaging-Konfiguration, Workflows zur proaktiven Reaktion und allgemeine Hinweise zur Sicherheitslage. Wählen Sie für diese Zwecke den Falltyp „Ermittlungen und Anfragen“ aus.

Wann sollten Sie Kontakt aufnehmen AWS Security Incident Response

Je nach Ihren Bedürfnissen können Sie AWS Security Incident Response für verschiedene Zwecke kontaktieren. In der folgenden Tabelle werden die verschiedenen Szenarien und die jeweils passende Kontaktmethode beschrieben.

Szenario	Wann sollte dies verwendet werden?	Reaktionszeit	Art des Falls
Aktiver Sicherheitsvorfall	Sie haben einen dringenden Sicherheitsvorfall, der sofortige Unterstützung und Services zur Reaktion auf den Vorfall erfordert	15 Minuten (erste Antwort)	Aktiver Sicherheitsvorfall
Untersuchung	Sie haben einen Sicherheitsvorfall erkannt und benötigen Unterstützung bei der Protokollanalyse und der sekundären Bestätigung der Untersuchung des Vorfalls	15 Minuten (erste Antwort)	Ermittlungen und Anfragen
Anfragen und Anleitungen	Sie haben Fragen zu GuardDuty Amazon-Ergebnissen, Unterdrückungsregeln, Alert-Triaging-Konfigurationen, Workflows zur proaktiven Reaktion oder	15 Minuten (erste Antwort)	Ermittlungen und Anfragen

Szenario	Wann sollte dies verwendet werden?	Reaktionszeit	Art des Falls
	zur allgemeinen Sicherheitslage in Bezug auf Funktionen AWS Security Incident Response		
Probleme beim Onboarding	Sie haben während des Onboarding-Prozesses für AWS Security Incident Response technische Probleme	Variiert je nach Supportplan	AWS Support Fall

Bei allen AWS unterstützten Fällen (aktiver Sicherheitsvorfall und Ermittlungen und Anfragen) antworten die Techniker für die Reaktion auf AWS Sicherheitsvorfälle innerhalb von 15 Minuten, um eine erste Antwort zu erhalten. Diese Reaktionszeit gilt nur für den ersten Kontakt und nicht für nachfolgende Antworten.

Das folgende Beispiel behandelt die Verwendung der Konsole.

1. Melden Sie sich AWS Security Incident Response über das an AWS-Managementkonsole.
2. Wählen Sie Create Case
3. Wählen Sie Fall lösen mit AWS
4. Wählen Sie die Art der Anfrage
   a. Aktiver Sicherheitsvorfall: Dieser Typ ist für Support und Services zur Reaktion auf dringende Vorfälle vorgesehen.
   b. Untersuchungen und Anfragen: Verwenden Sie diesen Typ für festgestellte Sicherheitsvorfälle, bei denen die Techniker für die Reaktion auf AWS Sicherheitsvorfälle Sie bei der Protokollanalyse und der sekundären Bestätigung der Untersuchung von Sicherheitsvorfällen unterstützen können. Sie können diesen Typ auch für Anfragen zu GuardDuty Ergebnissen, Unterdrückungsregeln, Alert-Triaging-Konfigurationen, proaktiven Reaktionsabläufen und allgemeinen Fragen zur Sicherheitslage im Zusammenhang mit den Funktionen zur Reaktion auf AWS Sicherheitsvorfälle verwenden.

5. Geben Sie als voraussichtliches Startdatum das Datum an, an dem Sie den Vorfall am frühesten erkannt haben. Zum Beispiel, wenn Sie zum ersten Mal ungewöhnliches Verhalten festgestellt haben oder als Sie die erste entsprechende Sicherheitswarnung erhalten haben.
6. Definieren Sie einen Titel für den Fall
7. Geben Sie eine detaillierte Beschreibung des Falls an. Beachten Sie die folgenden Aspekte, die Einsatzkräften bei der Lösung des Falls helfen können:
    a. Was ist passiert?
    b. Wer hat den Vorfall entdeckt und gemeldet?
    c. Wer ist von dem Fall betroffen?
    d. Was sind die bekannten Auswirkungen?
    e. Was ist die Dringlichkeit dieses Falls?
    f. Fügen Sie einen oder mehrere hinzu AWS-Konto IDs , die in den Anwendungsbereich des Falls fallen.
8. Fügen Sie optionale Falldetails hinzu:
    a. Wählen Sie aus der Drop-down-Liste die wichtigsten Dienste aus, die betroffen sind.
    b. Wählen Sie aus der Drop-down-Liste die wichtigsten betroffenen Regionen aus.
    c. Fügen Sie eine oder mehrere IP-Adressen von Bedrohungsakteuren hinzu, die Sie im Rahmen dieses Falls identifiziert haben.
9. Fügen Sie dem Fall optionale zusätzliche Incident-Responder hinzu, die Benachrichtigungen erhalten. Gehen Sie wie folgt vor, um eine Person hinzuzufügen:
    a. Fügen Sie eine E-Mail-Adresse hinzu.
    b. Fügen Sie optional einen Vor- und Nachnamen hinzu.
    c. Wählen Sie Neu hinzufügen, um eine weitere Person hinzuzufügen.
    d. Um eine Person zu entfernen, wählen Sie die Option Entfernen für eine Person.
    e. Wählen Sie „Hinzufügen“, um alle aufgelisteten Personen zum Fall hinzuzufügen.
        i. Sie können mehrere Personen auswählen und auf Entfernen klicken, um sie aus der Liste zu löschen.
10. Fügen Sie dem Fall optionale Tags hinzu.
    a. Führen Sie die folgenden Schritte aus, um ein Tag hinzuzufügen:
    b. Wählen Sie Neues Tag hinzufügen aus.
    c. Geben Sie unter Schlüssel den Namen des Tags ein.
    d. Geben Sie für Wert den Tag-Wert ein.

e. Um ein Tag zu entfernen, wählen Sie die Option Entfernen für dieses Tag.

Nachdem ein AWS unterstützter Fall erstellt wurde, werden die AWS Security Incident Response Engineers und Ihr Incident Response Team sofort benachrichtigt.

Um einen Fall mit AWS KI-gestützter Untersuchung zu erstellen

1. Öffnen Sie die AWS Security Incident Response Konsole unter console.aws.amazon.com/.
2. Wählen Sie im Navigationsbereich die Option Fälle aus.
3. Wählen Sie Create case (Fall erstellen) aus.
4. Wählen Sie als Falltyp die Option AWS-unterstützter Fall aus.
5. Geben Sie Falldetails an, einschließlich Titel, Startdatum des Vorfalls und AWS Konto-ID der betroffenen Person.
6. Geben Sie im Abschnitt „Beschreibung des Sicherheitsereignisses“ eine ausführliche Beschreibung des Vorfalls ein.
7. Geben Sie zusätzliche Informationen zu den betroffenen AWS Diensten, Regionen und anderen relevanten Details an.
8. Wählen Sie Create case (Fall erstellen) aus.

Nach der Erstellung des Falls beginnen sowohl die Security Incident Response-Techniker als auch der KI-Agent gleichzeitig mit der Arbeit.

Um auf klärende Fragen zur KI zu antworten (optional)

1. Navigieren Sie in Ihrem Fall zur Registerkarte Untersuchung.
2. Überprüfe alle klärenden Fragen, die dir der KI-Agent gestellt hat.
3. Beantworten Sie die Fragen oder wählen Sie Überspringen, wenn Sie nicht antworten möchten.
4. Wählen Sie Absenden, um fortzufahren. Alle Felder sind optional.

Verantwortungsvolle Offenlegung von KI

Zusammenfassungen von Untersuchungen werden mithilfe AWS generativer KI-Funktionen erstellt. Sie sind dafür verantwortlich, KI-generierte Empfehlungen in Ihrem spezifischen Kontext zu bewerten, geeignete Aufsichtsmechanismen zu implementieren, die Ergebnisse unabhängig zu verifizieren und die menschliche Aufsicht über alle Sicherheitsentscheidungen aufrechtzuerhalten.

Erstellen Sie einen selbst verwalteten Fall

Sie können ein selbstverwaltetes Formular AWS Security Incident Response über die Konsole, die API oder erstellen. AWS Command Line Interface Bei dieser Art von Fall sind die AWS Security Incident Response Engineers NICHT involviert. Das folgende Beispiel behandelt die Verwendung der Konsole.

1. Melden Sie sich AWS Security Incident Response über die Adresse AWS-Managementkonsole an https://console.aws.amazon.com/security-ir/.
2. Wählen Sie Create Case (Fall erstellen) aus.
3. Wählen Sie „Fall mit meinem eigenen Incident-Response-Team lösen“.
4. Geben Sie als voraussichtliches Startdatum das Datum an, an dem Sie den Vorfall am frühesten erkannt haben. Zum Beispiel, wenn Sie zum ersten Mal ungewöhnliches Verhalten festgestellt haben oder als Sie die erste entsprechende Sicherheitswarnung erhalten haben.
5. Definieren Sie einen Titel für den Fall. Es wird empfohlen, die Daten in den Falltitel aufzunehmen, wie es bei der Auswahl der Option „Titel generieren“ vorgeschlagen wurde.
6. Geben Sie an AWS-Konto IDs , dass sie Teil des Falls sind. Gehen Sie wie folgt vor, um eine Konto-ID hinzuzufügen:
   a. Geben Sie die 12-stellige Konto-ID ein und wählen Sie Konto hinzufügen.
   b. Um ein Konto zu entfernen, wählen Sie neben dem Konto, das Sie aus dem Fall entfernen möchten, die Option Entfernen aus.
7. Geben Sie eine detaillierte Beschreibung des Falls ein.
   a. Beachten Sie die folgenden Aspekte, die Einsatzkräften bei der Lösung des Falls helfen können:
      i. Was ist passiert?
      ii. Wer hat den Vorfall entdeckt und gemeldet?
      iii. Wer ist von dem Fall betroffen?
      iv. Was sind die bekannten Auswirkungen?
      v. Was ist die Dringlichkeit dieses Falls?
8. Fügen Sie optionale Falldetails hinzu:
   a. Wählen Sie aus der Drop-down-Liste die wichtigsten Dienste aus, die betroffen sind.
   b. Wählen Sie aus der Drop-down-Liste die wichtigsten betroffenen Regionen aus.
   c. Fügen Sie eine oder mehrere IP-Adressen von Bedrohungsakteuren hinzu, die Sie im Rahmen dieses Falls identifiziert haben.

9. Fügen Sie dem Fall optionale zusätzliche Incident-Responder hinzu, die Benachrichtigungen erhalten. Gehen Sie wie folgt vor, um eine Person hinzuzufügen:
   a. Fügen Sie eine E-Mail-Adresse hinzu.
   b. Fügen Sie optional einen Vor- und Nachnamen hinzu.
   c. Wählen Sie Neu hinzufügen, um eine weitere Person hinzuzufügen.
   d. Um eine Person zu entfernen, wählen Sie die Option Entfernen für eine Person.
   e. Wählen Sie „Hinzufügen“, um alle aufgelisteten Personen zum Fall hinzuzufügen. Sie können mehrere Personen auswählen und auf Entfernen klicken, um sie aus der Liste zu löschen.
10. Fügen Sie dem Fall optionale Tags hinzu. Führen Sie die folgenden Schritte aus, um ein Tag hinzuzufügen:
   a. Wählen Sie Neues Tag hinzufügen aus.
   b. Geben Sie unter Schlüssel den Namen des Tags ein.
   c. Geben Sie für Wert den Tag-Wert ein.
   d. Um ein Tag zu entfernen, wählen Sie die Option Entfernen für dieses Tag.

Das Incident-Response-Team wird nach der Erstellung des Falls per E-Mail benachrichtigt.

Zusammenarbeit mit Technikern für die Reaktion auf AWS Sicherheitsvorfälle

Nachdem Sie einen Sicherheitsvorfall eröffnet haben, beginnen die AWS Security Incident Response Engineers mit der Bearbeitung Ihres Vorfalls. In diesem Abschnitt wird erklärt, was Sie bei der Untersuchung erwartet und wie Sie effektiv mit unserem Team zusammenarbeiten können.

Was Sie von den AWS Security Incident Response-Technikern erwarten können

Wenn Sie einen AWS unterstützten Fall öffnen, wird Ihrem Vorfall ein Security Incident Response Engineer zugewiesen. Ihr zugewiesener Responder wird:

- Überprüfen Sie die ursprünglichen Informationen, die Sie in dem Fall angegeben haben
- Analysieren Sie relevante AWS Serviceprotokolle und Sicherheitsergebnisse
- Identifizieren Sie den Umfang und die Auswirkungen des Sicherheitsvorfalls
- Entwickeln Sie einen auf Ihre Situation zugeschnittenen Untersuchungs- und Reaktionsplan

Reaktionszeit: Das Service Level Objective (SLO) für die Bestätigung neuer Fälle durch AWS Security Incident Response Techniker liegt innerhalb von 15 Minuten. Der Zeitplan für die erste

Bewertung kann je nach Schweregrad und Komplexität des Falls variieren. Wenn die AWS Security Incident Response Techniker innerhalb von 5 Werktagen keine Antwort oder wichtige Informationen von Ihnen erhalten, ist der Fall abgeschlossen.

Arbeitsablauf bei der Untersuchung

AWS Die Techniker für die Reaktion auf Sicherheitsvorfälle folgen einem strukturierten Prozess zur Reaktion auf Vorfälle, der auf das NIST 800-61r2-Framework abgestimmt ist. Während Ihrer Untersuchung können Sie mit den folgenden Phasen rechnen:

1. Erste Prüfung — Die Techniker für die Reaktion auf Sicherheitsvorfälle überprüfen Ihre Falldetails und bestätigen den Umfang des Vorfalls
2. Untersuchung — Die Techniker für die Reaktion auf Sicherheitsvorfälle analysieren Protokolle, identifizieren Anzeichen für eine Gefährdung und ermitteln die Ursache
3. Eindämmung — Die Experten für die Reaktion auf Sicherheitsvorfälle empfehlen Maßnahmen, um die Auswirkungen des Vorfalls zu begrenzen
4. Beseitigung und Wiederherstellung — Die Security Incident Response-Techniker helfen Ihnen dabei, Bedrohungen zu entfernen und den normalen Betrieb wiederherzustellen
5. Überprüfung nach dem Vorfall — Die Experten für die Reaktion auf Sicherheitsvorfälle geben Erkenntnisse und Empfehlungen zur Vermeidung future Vorfälle

Während dieser Phasen hält Sie Ihr Security Incident Response Engineer über Fallaktualisierungen auf dem Laufenden und kann zusätzliche Informationen oder Maßnahmen von Ihnen anfordern.

Techniker für die Reaktion auf Informationssicherheitsvorfälle können folgende Anfragen stellen

Um Ihren Vorfall effektiv untersuchen zu können, bitten Sie die Techniker für die Reaktion auf AWS Sicherheitsvorfälle möglicherweise um folgende Angaben:

- Angaben zum Zeitplan — Wann Sie den Vorfall und alle relevanten Ereignisse, die dazu geführt haben, zum ersten Mal entdeckt haben
- Betroffene Ressourcen — Spezifisches AWS Konto IDs, Dienste, Regionen und ARNs beteiligte Ressourcen
- Zugriffsinformationen — Einzelheiten darüber, wer Zugriff auf die betroffenen Ressourcen hat, sowie alle kürzlich erfolgten Zugriffsänderungen
- Geschäftlicher Kontext — Wie die betroffenen Ressourcen genutzt werden und welche potenziellen Auswirkungen dies auf das Unternehmen hat

- Protokolle und Beweise — Zusätzliche Protokolle, Screenshots oder Artefakte, die bei der Untersuchung hilfreich sein könnten
- Autorisierung — Genehmigung zur Durchführung bestimmter Eindämmungs- oder Sanierungsmaßnahmen in Ihrem Namen

Ihr Security Incident Response Engineer erklärt Ihnen, warum die einzelnen Informationen benötigt werden und wie sie bei der Untersuchung helfen.

Bewährte Methoden im Bereich Kommunikation

Effektive Kommunikation beschleunigt die Lösung von Vorfällen. Beachten Sie bei der Zusammenarbeit mit AWS Security Incident Response-Technikern die folgenden Vorgehensweisen:

- Reagieren Sie umgehend auf Informationsanfragen Ihres Security Incident Response Engineers
- Geben Sie vollständige Informationen an, auch wenn Sie sich nicht sicher sind, ob sie relevant sind
- Stellen Sie Fragen, wenn Sie eine Empfehlung nicht verstehen oder weitere Informationen benötigen
- Informieren Sie den Fall über alle neuen Entwicklungen oder Änderungen des Vorfalls
- Benennen Sie einen Hauptansprechpartner aus Ihrem Team, der sich mit den Security Incident Response-Technikern abstimmt

> **Important**
>
> Wenn AWS Security Incident Response Techniker innerhalb von 5 Werktagen keine Antwort auf Anfragen zu wichtigen Informationen erhalten, bemühen wir uns, den Fall abzuschließen. Sie können einen Fall erneut öffnen, wenn neue Informationen verfügbar werden.

Ihre Rolle bei der Untersuchung

Während die AWS Security Incident Response Ingenieure die Untersuchung leiten, ist Ihre Teilnahme unerlässlich. Sie sind für die folgenden Aktionen verantwortlich:

- Rechtzeitige Beantwortung von Informationsanfragen
- Implementierung der empfohlenen Eindämmungs- und Problembehebungsmaßnahmen in Ihrer Umgebung AWS

- Autorisierung der Security Incident Response-Techniker, in Ihrem Namen Maßnahmen zu ergreifen (sofern Sie die proaktive Reaktion aktiviert haben)
- Abstimmung mit Ihren internen Teams (Sicherheit, Recht, Compliance) nach Bedarf
- Treffen von Geschäftsentscheidungen über Prioritäten und Kompromisse bei der Reaktion auf Vorfälle

AWS Security Incident Response Techniker bieten Fachwissen und Empfehlungen, aber Sie behalten die Kontrolle über Ihre AWS Ressourcen und treffen die endgültigen Entscheidungen über Reaktionsmaßnahmen.

Abschluss des Falls

AWS Security Incident Response Techniker schließen Ihren Fall ab, wenn:

- Der Vorfall wurde eingedämmt und behoben
- Alle Ergebnisse der Untersuchung wurden mit Ihnen geteilt
- Es ist keine weitere Unterstützung durch einen Security Incident Response Engineer erforderlich
- Sie beantragen den Abschluss des Falls

Bevor Sie einen Fall abschließen, gibt Ihnen Ihr Security Incident Response Engineer eine Zusammenfassung der Ergebnisse, ergriffenen Maßnahmen und Empfehlungen zur Verbesserung Ihrer Sicherheitslage.

Wenn Sie nach Abschluss des Falls weitere Unterstützung benötigen, können Sie einen neuen Fall eröffnen oder Kontakt aufnehmen AWS Support.

Auf einen AWS generierten Fall antworten

AWS Security Incident Response kann zu einer ausgehenden Benachrichtigung oder einem Fall führen, wenn Sie auf etwas reagieren müssen oder sich dessen bewusst sein müssen, das sich möglicherweise auf Ihr Konto oder Ihre Ressourcen auswirkt. Dies ist nur der Fall, wenn Sie die Workflows proaktive Reaktion und Alert-Triaging als Teil Ihres Abonnements aktiviert haben.

Diese Benachrichtigungen werden in der AWS Security Incident Response Konsole als Security Incident Response-Fälle mit dem Präfix „[Proactive case]“ angezeigt. Gehen Sie wie folgt vor, um diese Fälle anzuzeigen und zu verwalten:

- Öffnen Sie die Security Incident Response-Konsole unter https://console.aws.amazon.com/security-ir/

- Wählen Sie Fälle aus.
- Sie sehen alle Fälle, einschließlich der Fälle mit dem Präfix „[Proaktiver Fall]“.

Sie können diese Fälle nach Bedarf aktualisieren, lösen und erneut öffnen. In diesen Fällen können Sie direkt mit dem AWS Security Incident Response Team kommunizieren und so eine effiziente Behandlung potenzieller Sicherheitsprobleme sicherstellen.

Fälle verwalten

Inhalt

Den Fallstatus ändern

Ein Fall befindet sich in einem der folgenden Staaten:

- Eingereicht: Dies ist der ursprüngliche Status eines Falls. Fälle in diesem Status wurden von einer angefragten Person eingereicht, werden aber noch nicht bearbeitet.
- Erkennung und Analyse: Dieser Status zeigt an, dass ein Incident-Responder mit der Bearbeitung des Falls begonnen hat. Diese Phase umfasst die Erfassung von Daten, die Einstufung des Ereignisses und die Durchführung von Analysen, um datengestützte Schlussfolgerungen zu ziehen.
- Eindämmung, Beseitigung und Wiederherstellung: In diesem Status hat der Incident Responder verdächtige Aktivitäten identifiziert, deren Beseitigung zusätzlichen Aufwand erfordert. Der Incident Responder gibt Ihnen Empfehlungen für die Analyse des Geschäftsrisikos und weitere Maßnahmen. Wenn Sie die Opt-in-Funktionen für den Service aktiviert haben, wird ein AWS

Incident Responder Sie um Ihre Zustimmung bitten, Eindämmungsmaßnahmen anhand von SSM-Dokumenten in den betroffenen Konten durchzuführen.

- Aktivitäten nach dem Vorfall: In diesem Status wurde das primäre Sicherheitsereignis eingedämmt. Der Schwerpunkt liegt nun auf der Wiederherstellung und Wiederherstellung des normalen Geschäftsbetriebs. Wenn der Resolver für den Fall unterstützt wird, werden eine Zusammenfassung und eine AWS Ursachenanalyse bereitgestellt.
- Geschlossen: Dies ist der endgültige Status des Workflows. Fälle mit dem Status „Abgeschlossen“ weisen darauf hin, dass die Arbeit abgeschlossen wurde. Geschlossene Fälle können nicht erneut geöffnet werden. Stellen Sie daher sicher, dass alle Aktionen abgeschlossen sind, bevor Sie zu diesem Status wechseln.

Wählen Sie Aktion/Status aktualisieren, um den Status des Falls für selbst verwaltete Fälle zu ändern. Bei AWS unterstützten Fällen wird der Status von den AWS Security Incident Response-Technikern festgelegt.

Den Resolver ändern

Bei selbst verwalteten Fällen kann Ihr Incident-Response-Team Hilfe von anfordern. AWS Wählen Sie Hilfe anfordern von AWS, um den Resolver für diesen Fall auf zu ändern. AWS Sobald der Fall auf „ AWS Unterstützt“ aktualisiert wurde, wird der Status in „Eingereicht“ geändert. Die bestehende Fallhistorie wird den Technikern von AWS Security Incident Response zur Verfügung stehen. Sobald Sie Hilfe von angefordert haben, können AWS Sie diese nicht mehr auf „Selbstverwaltung“ umstellen.

Aktionselemente

Ein Techniker für die Reaktion auf AWS Sicherheitsvorfälle, der an dem Fall arbeitet, kann Ihr internes Team um Maßnahmen bitten.

Zu den Aktionselementen, die nach der Erstellung eines Falls angezeigt werden, gehören:

- Anfrage, einem Incident-Responder die Erlaubnis zu erteilen, auf einen Fall zuzugreifen
- Bitte um weitere Informationen zu dem Fall

Aktionspunkte, wenn ein Fall zum Abschluss bereit ist:

- Bitte um Überprüfung des Fallberichts
- Antrag auf Abschluss des Falls

Bearbeiten eines Falls

Wählen Sie Bearbeiten, um die Details eines Falls zu ändern.

Für AWS unterstützte und selbst verwaltete Fälle:

Sie können die folgenden Falldetails ändern, nachdem ein Fall erstellt wurde:

- Title
- Description

Nur für AWS unterstützte Fälle:

Sie können die zusätzlichen Felder ändern:

- Typ der Anforderung:
  - Aktiver Sicherheitsvorfall: Dieser Typ ist für Support und Services zur Reaktion auf dringende Vorfälle vorgesehen.
  - Untersuchungen: Untersuchungen ermöglichen es Ihnen, Unterstützung bei festgestellten Sicherheitsvorfällen zu erhalten, wobei die AWS Security Incident Response Engineers Sie bei der Protokollierung und sekundären Bestätigung des Sicherheitsvorfalls unterstützen können.
- Voraussichtliches Startdatum: Ändern Sie dieses Feld, wenn Sie für diesen Fall Indikatoren erhalten haben, die vor dem ursprünglich angegebenen Startdatum liegen. Erwägen Sie, zusätzliche Details zu dem neu erkannten Indikator im Beschreibungsfeld anzugeben oder auf der Registerkarte Kommunikation einen Kommentar hinzuzufügen.

Kommunikation

AWS Security Incident Response-Techniker können Kommentare hinzufügen, um ihre Aktivitäten bei der Bearbeitung eines Falls zu dokumentieren. Verschiedene AWS Security Incident Response-Techniker können gleichzeitig an einem Fall arbeiten. Sie werden im Kommunikationsprotokoll als AWS Responder dargestellt.

Berechtigungen

Auf der Registerkarte „Berechtigungen“ sind alle Personen aufgeführt, die bei jeder Änderung des Falls benachrichtigt werden. Sie können Personen zur Liste hinzufügen und daraus entfernen, bis der Fall abgeschlossen ist.

> **Note**
>
> In Einzelfällen können Sie insgesamt bis zu 30 Interessengruppen einbeziehen. Um diesen Stakeholdern Zugriff auf Fallebene zu gewähren, ist eine zusätzliche Berechtigungskonfiguration erforderlich.

Gewähren Sie Zugriff auf einen Fall in der Konsole

Um Zugriff auf den Fall in der zu gewähren AWS-Managementkonsole, können Sie die Vorlage für die IAM-Berechtigungsrichtlinie kopieren und diese Berechtigung einem Benutzer oder einer Rolle hinzufügen.

Hinzufügen der IAM-Richtlinie zu einem Benutzer oder einer Rolle:

1. Kopieren Sie die IAM-Berechtigungsrichtlinie.
2. Öffnen Sie IAM in der Via. https://console.aws.amazon.com/iam/
3. Wählen Sie im Navigationsbereich Benutzer oder Rollen aus.
4. Wählen Sie einen Benutzer oder eine Rolle aus, um die Detailseite zu öffnen.
5. Wählen Sie auf der Registerkarte „Berechtigungen“ die Option „Berechtigungen hinzufügen“ aus.
6. Wählen Sie Richtlinie anfügen aus.
7. Wählen Sie die entsprechende AWS Security Incident Response verwaltete Richtlinie aus.
8. Wählen Sie Richtlinie hinzufügen aus.

Anlagen

Ihre Incident-Responder können einem Fall Anlagen hinzufügen, die anderen Incident-Respondern bei der Untersuchung selbst verwalteter Fälle helfen.

> **Note**
>
> Wenn Sie sich für einen AWS unterstützten Fall entscheiden, können keine Anlagen angezeigt werden. AWS Alle Informationen zu AWS unterstützten Fällen müssen in Form von Fallkommentaren oder durch die Bereitstellung eines Screenshots mit Ihrer bevorzugten Kommunikationstechnologie geteilt werden.

Wählen Sie Hochladen, um eine Datei von Ihrem Computer auszuwählen, die dem Fall hinzugefügt werden soll.

> **Note**
>
> Alle hochgeladenen Anlagen werden sieben Tage nach Abschluss eines Falls gelöscht`Closed`.

Tags (Markierungen)

Ein Tag ist eine optionale Bezeichnung, die Sie Ihren Fällen zuweisen können, um Metadaten zu dieser Ressource zu speichern. Jedes Tag ist eine Bezeichnung, die aus einem Schlüssel und einem optionalen Wert besteht. Sie können Tags verwenden, um nach Ressourcen zu suchen, Kosten zuzuweisen und Berechtigungen zu authentifizieren.

Führen Sie die folgenden Schritte aus, um ein Tag hinzuzufügen:

1. Wählen Sie Neues Tag hinzufügen aus.
2. Geben Sie unter Schlüssel den Namen des Tags ein.
3. Geben Sie für Wert den Tag-Wert ein.

Um ein Tag zu entfernen, wählen Sie die Option Entfernen für dieses Tag.

Fallaktivitäten

Prüfprotokolle bieten detaillierte chronologische Aufzeichnungen aller Fallaktivitäten. Sie liefern wichtige Informationen für Aktivitäten nach der Veranstaltung und helfen dabei, Verbesserungspotenziale zu identifizieren. Die Uhrzeit, der Benutzer, die Aktion und die Einzelheiten aller Falländerungen werden im Fallprüfprotokoll protokolliert.

Einen Fall schließen

Wählen Sie für AWS unterstützte Fälle auf der Seite mit den Falldetails die Option „Fall schließen“, um den Fall in einem beliebigen Status dauerhaft zu schließen. Ein Fall erreicht in der Regel den Status Bereit zum Abschluss, bevor er dauerhaft geschlossen ist. Wenn Sie einen Fall vorzeitig mit einem anderen Status als Bereit zum Abschluss schließen, bitten Sie die Techniker für die Reaktion auf AWS Sicherheitsvorfälle, die Bearbeitung dieses AWS unterstützten Falls einzustellen.

Wenn Ihr Incident-Response-Team der Responder ist, wählen Sie auf der Seite mit den Falldetails die Option Aktion/Fall schließen aus.

> **Note**
>
> Der Status „Bereit zum Abschluss“ bedeutet, dass ein Fall dauerhaft abgeschlossen werden kann und dass an einem Fall keine weiteren Arbeiten erforderlich sind.

Ein Fall kann nicht erneut geöffnet werden, nachdem er dauerhaft geschlossen wurde. Alle Informationen werden schreibgeschützt verfügbar sein. Um ein versehentliches Schließen zu verhindern, werden Sie aufgefordert, zu bestätigen, dass Sie das Gehäuse schließen möchten.

Arbeitet mit CloudFormation StackSets

> **Important**
>
> AWS Security Incident Response aktiviert standardmäßig keine Containment-Funktionen. Um diese Containment-Aktionen auszuführen, müssen Sie dem Service mithilfe AWS Identity and Access Management von Rollen die erforderlichen Berechtigungen erteilen. Sie können diese Rollen einzeln für jedes Konto oder für Ihre gesamte Organisation StackSets erstellen CloudFormation StackSets, indem Sie die erforderlichen Rollen bereitstellen.

Spezifische Anweisungen zum Erstellen einer StackSet mit vom Dienst verwalteten Berechtigungen finden Sie unter Erstellen CloudFormation StackSets mit vom Dienst verwalteten Berechtigungen im AWS CloudFormation Benutzerhandbuch.

Im Folgenden finden Sie Vorlagen zum Erstellen der Rollen AWSSecurityIncidentResponseContainmentund AWSSecurityIncidentResponseContainmentExecution.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for production SIR containment roles'

Resources:
  AWSSecurityIncidentResponseContainment:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainment
```

```
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:AssumeRole',
                'Condition': { 'StringEquals': { 'sts:ExternalId': !Sub
 '${AWS::AccountId}' } },
              },
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:TagSession',
              },
            ],
        }
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentPolicy
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
                [
                  {
                    'Effect': 'Allow',
                    'Action': ['ssm:StartAutomationExecution'],
                    'Resource':
                      [
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainEC2Instance:$DEFAULT',
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainS3Resource:$DEFAULT',
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainIAMPrincipal:$DEFAULT',
                      ],
                  },
                  {
                    'Effect': 'Allow',
                    'Action':
                      ['ssm:DescribeInstanceInformation', 'ssm:GetAutomationExecution',
 'ssm:ListCommandInvocations'],
```

```
                  'Resource': '*',
                },
                {
                  'Effect': 'Allow',
                  'Action': ['iam:PassRole'],
                  'Resource': !GetAtt
AWSSecurityIncidentResponseContainmentExecution.Arn,
                  'Condition': { 'StringEquals': { 'iam:PassedToService':
'ssm.amazonaws.com' } },
                },
              ],
          }
 AWSSecurityIncidentResponseContainmentExecution:
   Type: 'AWS::IAM::Role'
   Properties:
     RoleName: AWSSecurityIncidentResponseContainmentExecution
     AssumeRolePolicyDocument:
       {
         'Version': '2012-10-17',
         'Statement':
           [{ 'Effect': 'Allow', 'Principal': { 'Service': 'ssm.amazonaws.com' },
'Action': 'sts:AssumeRole' }],
       }
     ManagedPolicyArns:
       - !Sub arn:${AWS::Partition}:iam::aws:policy/SecurityAudit
     Policies:
       - PolicyName: AWSSecurityIncidentResponseContainmentExecutionPolicy
         PolicyDocument:
           {
             'Version': '2012-10-17',
             'Statement':
               [
                 {
                   'Sid': 'AllowIAMContainment',
                   'Effect': 'Allow',
                   'Action':
                     [
                       'iam:AttachRolePolicy',
                       'iam:AttachUserPolicy',
                       'iam:DeactivateMFADevice',
                       'iam:DeleteLoginProfile',
                       'iam:DeleteRolePolicy',
                       'iam:DeleteUserPolicy',
                       'iam:GetLoginProfile',
```

```
                'iam:GetPolicy',
                'iam:GetRole',
                'iam:GetRolePolicy',
                'iam:GetUser',
                'iam:GetUserPolicy',
                'iam:ListAccessKeys',
                'iam:ListAttachedRolePolicies',
                'iam:ListAttachedUserPolicies',
                'iam:ListMfaDevices',
                'iam:ListPolicies',
                'iam:ListRolePolicies',
                'iam:ListUserPolicies',
                'iam:ListVirtualMFADevices',
                'iam:PutRolePolicy',
                'iam:PutUserPolicy',
                'iam:TagMFADevice',
                'iam:TagPolicy',
                'iam:TagRole',
                'iam:TagUser',
                'iam:UntagMFADevice',
                'iam:UntagPolicy',
                'iam:UntagRole',
                'iam:UntagUser',
                'iam:UpdateAccessKey',
                'identitystore:CreateGroupMembership',
                'identitystore:DeleteGroupMembership',
                'identitystore:IsMemberInGroups',
                'identitystore:ListUsers',
                'identitystore:ListGroups',
                'identitystore:ListGroupMemberships',
            ],
          'Resource': '*',
        },
        {
          'Sid': 'AllowOrgListAccounts',
          'Effect': 'Allow',
          'Action': 'organizations:ListAccounts',
          'Resource': '*',
        },
        {
          'Sid': 'AllowSSOContainment',
          'Effect': 'Allow',
          'Action':
            [
```

```
                        'sso:CreateAccountAssignment',
                        'sso:DeleteAccountAssignment',
                        'sso:DeleteInlinePolicyFromPermissionSet',
                        'sso:GetInlinePolicyForPermissionSet',
                        'sso:ListAccountAssignments',
                        'sso:ListInstances',
                        'sso:ListPermissionSets',
                        'sso:ListPermissionSetsProvisionedToAccount',
                        'sso:PutInlinePolicyToPermissionSet',
                        'sso:TagResource',
                        'sso:UntagResource',
                    ],
                  'Resource': '*',
                },
                {
                  'Sid': 'AllowSSORead',
                  'Effect': 'Allow',
                  'Action': ['sso-directory:SearchUsers', 'sso-
directory:DescribeUser'],
                  'Resource': '*',
                },
                {
                  'Sid': 'AllowS3Read',
                  'Effect': 'Allow',
                  'Action':
                    [
                      's3:GetAccountPublicAccessBlock',
                      's3:GetBucketAcl',
                      's3:GetBucketLocation',
                      's3:GetBucketOwnershipControls',
                      's3:GetBucketPolicy',
                      's3:GetBucketPolicyStatus',
                      's3:GetBucketPublicAccessBlock',
                      's3:GetBucketTagging',
                      's3:GetEncryptionConfiguration',
                      's3:GetObject',
                      's3:GetObjectAcl',
                      's3:GetObjectTagging',
                      's3:GetReplicationConfiguration',
                      's3:ListBucket',
                      's3express:GetBucketPolicy',
                    ],
                  'Resource': '*',
                },
```

```
                    {
                      'Sid': 'AllowS3Write',
                      'Effect': 'Allow',
                      'Action':
                        [
                          's3:CreateBucket',
                          's3:DeleteBucketPolicy',
                          's3:DeleteObjectTagging',
                          's3:PutAccountPublicAccessBlock',
                          's3:PutBucketACL',
                          's3:PutBucketOwnershipControls',
                          's3:PutBucketPolicy',
                          's3:PutBucketPublicAccessBlock',
                          's3:PutBucketTagging',
                          's3:PutBucketVersioning',
                          's3:PutObject',
                          's3:PutObjectAcl',
                          's3express:CreateSession',
                          's3express:DeleteBucketPolicy',
                          's3express:PutBucketPolicy',
                        ],
                      'Resource': '*',
                    },
                    {
                      'Sid': 'AllowAutoScalingWrite',
                      'Effect': 'Allow',
                      'Action':
                        [
                          'autoscaling:CreateOrUpdateTags',
                          'autoscaling:DeleteTags',
                          'autoscaling:DescribeAutoScalingGroups',
                          'autoscaling:DescribeAutoScalingInstances',
                          'autoscaling:DescribeTags',
                          'autoscaling:EnterStandby',
                          'autoscaling:ExitStandby',
                          'autoscaling:UpdateAutoScalingGroup',
                        ],
                      'Resource': '*',
                    },
                    {
                      'Sid': 'AllowEC2Containment',
                      'Effect': 'Allow',
                      'Action':
                        [
```

```
                    'ec2:AuthorizeSecurityGroupEgress',
                    'ec2:AuthorizeSecurityGroupIngress',
                    'ec2:CopyImage',
                    'ec2:CreateImage',
                    'ec2:CreateSecurityGroup',
                    'ec2:CreateSnapshot',
                    'ec2:CreateTags',
                    'ec2:DeleteSecurityGroup',
                    'ec2:DeleteTags',
                    'ec2:DescribeImages',
                    'ec2:DescribeInstances',
                    'ec2:DescribeSecurityGroups',
                    'ec2:DescribeSnapshots',
                    'ec2:DescribeTags',
                    'ec2:ModifyNetworkInterfaceAttribute',
                    'ec2:RevokeSecurityGroupEgress',
                ],
              'Resource': '*',
            },
            {
              'Sid': 'AllowKMSActions',
              'Effect': 'Allow',
              'Action':
                [
                  'kms:CreateGrant',
                  'kms:DescribeKey',
                  'kms:GenerateDataKeyWithoutPlaintext',
                  'kms:ReEncryptFrom',
                  'kms:ReEncryptTo',
                ],
              'Resource': '*',
            },
            {
              'Sid': 'AllowSSMActions',
              'Effect': 'Allow',
              'Action': ['ssm:DescribeAutomationExecutions'],
              'Resource': '*',
            },
          ],
        }
```

Mitgliedschaft kündigen

Eine Rolle mit der CancelMembership entsprechenden Berechtigung AWS Security Incident Response kann die Mitgliedschaft über die Konsole, die API oder kündigen AWS Command Line Interface.

> **Important**
>
> Sobald eine Mitgliedschaft gekündigt wurde, können Sie keine historischen Falldaten mehr einsehen. Wenn Sie eine Mitgliedschaft kündigen, wird Ihre Mitgliedschaft sofort gelöscht und Sie haben keinen weiteren Zugriff mehr auf die Fälle in der Mitgliedschaft. Alle Ressourcen oder Untersuchungen, die bei Kündigung der Mitgliedschaft ebenfalls eingestellt wurden `Active` oder `ready to close` werden.

Wenn Sie eine Mitgliedschaft kündigen:

Ihre Mitgliedschaft wird gelöscht und Sie haben keinen weiteren Zugriff mehr auf die Fälle in der Mitgliedschaft.

> **Important**
>
> Wenn Sie den Service erneut abonnieren, wird eine neue Mitgliedschaft erstellt, und auf die Fallressourcen, die im Rahmen der vorherigen Mitgliedschaft gespeichert waren, kann nur zugegriffen werden, wenn Sie sie vor der Kündigung heruntergeladen haben.

Nach der Kündigung der Mitgliedschaft werden alle Mitglieder des Incident-Response-Teams per E-Mail benachrichtigt.

> **Important**
>
> Wenn Sie eine Mitgliedschaft mit einem delegierten Administratorkonto erstellt haben und die AWS Organizations API verwenden, um die Bezeichnung eines delegierten Administrators aus dem Konto zu entfernen, wird die Mitgliedschaft sofort beendet.

Ressourcen taggen AWS Security Incident Response

Ein Tag ist ein Metadaten-Label, das Sie zuweisen oder das einer AWS AWS Ressource zugewiesen wird. Jedes Tag besteht aus einem Schlüssel und einem Wert. Für Tags, die Sie zuweisen, definieren Sie einen Schlüssel und einen Wert. So können Sie beispielsweise den Schlüssel als `stage` und den Wert für eine Ressource als `test` definieren.

Tags sind für folgende Aktivitäten nützlich:

- Identifizieren und organisieren Sie Ihre AWS Ressourcen. Viele AWS-Services unterstützen Tagging, sodass Sie Ressourcen aus verschiedenen Diensten dasselbe Tag zuweisen können, um anzuzeigen, dass die Ressourcen miteinander verknüpft sind.
- Verfolgen Sie Ihre AWS Kosten. Sie aktivieren diese Tags auf dem AWS Billing Dashboard. AWS verwendet die Tags, um Ihre Kosten zu kategorisieren und Ihnen einen monatlichen Kostenverteilungsbericht zu senden. Weitere Informationen finden Sie unter Verwenden von Kostenzuordnungs-Tags im AWS Billing User Guide.
- Steuern Sie den Zugriff auf Ihre AWS Ressourcen. Weitere Informationen finden Sie unter Controlling access using tags (Zugriffssteuerung mit Tags) im IAM-Benutzerhandbuch.

Informationen zum Tagging finden Sie in der AWS Security Incident Response API-Referenz.

Wird verwendet AWS CloudShell , um mit AWS Security Incident Response zu arbeiten

AWS CloudShell ist eine browserbasierte, vorauthentifizierte Shell, die Sie direkt von der aus starten können. AWS-Managementkonsole Sie können AWS CLI Befehle für AWS Dienste (einschließlich AWS Security Incident Response) mithilfe Ihrer bevorzugten Shell (Bash PowerShell oder Z-Shell) ausführen. Und Sie können dies tun, ohne Befehlszeilentools herunterladen oder installieren zu müssen.

Sie starten AWS CloudShell von der aus AWS-Managementkonsole, und die AWS Anmeldeinformationen, mit denen Sie sich an der Konsole angemeldet haben, sind in einer neuen Shell-Sitzung automatisch verfügbar. Diese Vorauthentifizierung von AWS CloudShell Benutzern ermöglicht es Ihnen, die Konfiguration von Anmeldeinformationen zu überspringen, wenn Sie mit AWS Diensten wie Security Incident Response interagieren, die AWS CLI Version 2 verwenden (vorinstalliert in der Computerumgebung der Shell).

Inhalt

Erhalt von IAM-Berechtigungen für AWS CloudShell

Mithilfe der von bereitgestellten Ressourcen zur Zugriffsverwaltung können Administratoren IAM-Benutzern Berechtigungen erteilen AWS Identity and Access Management, sodass sie auf die Funktionen der Umgebung zugreifen AWS CloudShell und diese nutzen können.

Am schnellsten kann ein Administrator Benutzern Zugriff gewähren, indem er eine AWS verwaltete Richtlinie verwendet. Bei einer von AWS verwalteten Richtlinie handelt es sich um eine eigenständige Richtlinie, die von AWS erstellt und verwaltet wird. Die folgende AWS verwaltete Richtlinie für CloudShell kann an IAM-Identitäten angehängt werden:

- `AWSCloudShellFullAccess`: Erteilt die Erlaubnis zur Nutzung AWS CloudShell mit vollem Zugriff auf alle Funktionen.

Wenn Sie den Umfang der Aktionen einschränken möchten, die ein IAM-Benutzer ausführen kann AWS CloudShell, können Sie eine benutzerdefinierte Richtlinie erstellen, die die

`AWSCloudShellFullAccess` verwaltete Richtlinie als Vorlage verwendet. Weitere Informationen zur Einschränkung der Aktionen, die Benutzern zur Verfügung stehen CloudShell, finden Sie im AWS CloudShell Benutzerhandbuch unter Verwaltung von AWS CloudShell Zugriff und Nutzung mit IAM-Richtlinien.

> **Note**
>
> Für Ihre IAM-Identität ist außerdem eine Richtlinie erforderlich, die die Erlaubnis erteilt, Anrufe an Security Incident Response zu tätigen.

Interaktion mit Security Incident Response mithilfe von AWS CloudShell

Nach dem Start AWS CloudShell von der AWS-Managementkonsole aus können Sie sofort mit der Interaktion mit Security Incident Response über die Befehlszeilenschnittstelle beginnen.

> **Note**
>
> Wenn Sie AWS Command Line Interface in verwenden AWS CloudShell, müssen Sie keine zusätzlichen Ressourcen herunterladen oder installieren. Da Sie außerdem bereits in der Shell authentifiziert sind, müssen Sie vor dem Tätigen von Anrufen keine Anmeldeinformationen konfigurieren.

Arbeit mit Sicherheitsvorfällen AWS CloudShell und Reaktion auf Sicherheitsvorfälle

1. Starten Sie von der aus AWS-Managementkonsole, CloudShell indem Sie die folgenden Optionen wählen, die in der Navigationsleiste verfügbar sind:
   - Wählen Sie das CloudShell Symbol.
   - Beginnen Sie mit der Eingabe von „Cloudshell“ in das Suchfeld und wählen Sie dann die CloudShell Option.
2. Verwenden Sie den Standard AWS Command Line Interface , um mit AWS Security Incident Response zu interagieren. Eine vollständige Referenz der verfügbaren CLI-Befehle finden Sie in der AWS CLI Befehlsreferenz für die Reaktion auf AWS Sicherheitsvorfälle.

Protokollieren von AWS Security Incident Response API-Aufrufen mit AWS CloudTrail

AWS Security Incident Response ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen eines Benutzers, einer Rolle oder eines AWS Dienstes in Security Incident Response bereitstellt. CloudTrail erfasst alle API-Aufrufe für Security Incident Response als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Security Incident Response-Konsole und Code-Aufrufe an die Security Incident Response-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Security Incident Response. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf einsehen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Security Incident Response gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zur Reaktion auf Sicherheitsvorfälle finden Sie unter CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn in Security Incident Response eine Aktivität auftritt, wird diese Aktivität zusammen mit anderen CloudTrail AWS Serviceereignissen in der Ereignishistorie als Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in AWS-Konto den letzten 90 Tagen erstellen Sie einen Trail- oder CloudTrailLake-Event-Datenspeicher.

CloudTrail Pfade

> Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Alle mit dem erstellten Pfade AWS-Managementkonsole sind regionsübergreifend. Sie können mithilfe von AWS CLI einen Einzel-Region- oder einen Multi-Region-Trail erstellen. Es wird empfohlen, einen Trail mit mehreren Regionen zu erstellen, da Sie alle Aktivitäten AWS-Regionen in Ihrem Konto erfassen. Wenn Sie einen Einzel-Region-Trail erstellen, können Sie nur die Ereignisse anzeigen, die im AWS-Region des Trails protokolliert wurden. Weitere

Informationen zu Trails finden Sie unter Erstellen eines Trails für Ihr AWS-Konto und Erstellen eines Trails für eine Organisation im AWS CloudTrail -Benutzerhandbuch.

Sie können eine Kopie Ihrer laufenden Verwaltungsereignisse kostenlos an Ihren Amazon S3 S3-Bucket senden, CloudTrail indem Sie einen Trail erstellen. Es fallen jedoch Amazon S3 S3-Speichergebühren an. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise. Informationen zu Amazon-S3-Preisen finden Sie unter Amazon S3 – Preise.

CloudTrail Datenspeicher für Ereignisse in Lake

CloudTrail Mit Lake können Sie SQL-basierte Abfragen für Ihre Ereignisse ausführen. CloudTrail Lake konvertiert bestehende Ereignisse im zeilenbasierten JSON-Format in das Apache ORC-Format. ORC ist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von Daten optimiert ist. Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die Sie mit Hilfe von erweiterten Ereignisselektoren auswählen. Die Selektoren, die Sie auf einen Ereignisdatenspeicher anwenden, steuern, welche Ereignisse bestehen bleiben und für Sie zur Abfrage verfügbar sind. Weitere Informationen zu CloudTrail Lake finden Sie unter Arbeiten mit AWS CloudTrail Lake im AWS CloudTrail Benutzerhandbuch.

CloudTrail Für das Speichern und Abfragen von Ereignisdaten in Lake fallen Kosten an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Preisoption aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Weitere Informationen zur Preisgestaltung finden Sie unter CloudTrail AWS CloudTrail Preisgestaltung.

Alle Aktionen zur Reaktion auf Sicherheitsvorfälle werden von der AWS Security Incident Response API-Referenz protokolliert CloudTrail und sind dort dokumentiert. Beispielsweise generieren Aufrufe von `CreateCase` und `UpdateCase` Aktionen Einträge in den CloudTrail Protokolldateien. `CreateMembership`

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 Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.

- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Die Einträge der Security Incident Response-Protokolldatei verstehen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die CreateCase Aktion demonstriert.


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA00000000000000000:user",
        "arn": "arn:aws:sts::123412341234:assumed-role/Admin/user",
        "accountId": "123412341234",
        "accessKeyId": "****",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA00000000000000000",
                "arn": "arn:aws:iam::123412341234:role/Admin",
                "accountId": "123412341234",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-10-13T06:32:53Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-10-13T06:40:45Z",
    "eventSource": "security-ir.amazonaws.com",
```

```
    "eventName": "CreateCase",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "aws-cli/2.17.23 md/awscrt#0.20.11 ua/2.0 os/macos#23.6.0 md/
arch#x86_64 lang/python#3.11.9 md/pyimpl#CPython cfg/retry-mode#standard md/
installer#exe md/prompt#off md/command#security-ir.create-case",
    "requestParameters": {
        "impactedServices": [
            "Amazon GuardDuty"
        ],
        "impactedAccounts": [],
        "clientToken": "testToken112345679",
        "resolverType": "Self",
        "description": "***",
        "engagementType": "Investigation",
        "watchers": [
            {
                "email": "***",
                "name": "***",
                "jobTitle": "***"
            }
        ],
        "membershipId": "m-r1abcdabcd",
        "title": "***",
        "impactedAwsRegions": [
            {
                "region": "ap-southeast-1"
            }
        ],
        "reportedIncidentStartDate": 1711553521,
        "threatActorIpAddresses": [
            {
                "ipAddress": "***",
                "userAgent": "browser"
            }
        ]
    },
    "responseElements": {
        "caseId": "0000000001"
    },
    "requestID": "2db4b08d-94a9-457a-9474-5892e6c8191f",
    "eventID": "b3fa3990-db82-43be-b120-c81262cc2f19",
    "readOnly": false,
    "resources": [
```

```
        {
            "accountId": "123412341234",
            "type": "AWS::SecurityResponder::Case",
            "ARN": "arn:aws:security-ir:us-east-1:123412341234:case/*"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123412341234",
    "eventCategory": "Management"
}
```

AWS Security Incident Response Konten verwalten mit AWS Organizations

AWS Security Incident Response ist integriert in. AWS Organizations Das AWS Organizations Verwaltungskonto der Organisation kann ein Konto als delegierten Administrator für festlegen. AWS Security Incident Response Diese Aktion wird AWS Security Incident Response als vertrauenswürdiger Dienst in aktiviert. AWS Organizations Informationen darüber, wie diese Berechtigungen gewährt werden, finden Sie unter Zusammen AWS Organizations mit anderen AWS Diensten verwenden.

In den folgenden Abschnitten werden Sie durch verschiedene Aufgaben geführt, die Sie als delegiertes Security Incident Response-Administratorkonto ausführen können.

Inhalt

Überlegungen und Empfehlungen zur Verwendung mit AWS Security Incident Response AWS Organizations

Die folgenden Überlegungen und Empfehlungen können Ihnen helfen zu verstehen, wie ein delegiertes Security Incident Response-Administratorkonto funktioniert in: AWS Security Incident Response

Delegiertes Administratorkonto für. AWS Security Incident Response

Sie können ein Mitgliedskonto als delegiertes Security Incident Response-Administratorkonto festlegen. Wenn Sie beispielsweise ein Mitgliedskonto *111122223333* in angeben*Europe (Ireland)*, können Sie kein anderes Mitgliedskonto in angeben. *555555555555 Canada (Central)* In allen anderen Regionen müssen Sie dasselbe Konto wie das delegierte Administratorkonto für Security Incident Response verwenden.

Sie richten Ihr delegiertes Security Incident Response-Administratorkonto in einem bestimmten Bereich ein. AWS-Region

AWS-Region Bei der Ersteinrichtung weisen Sie ein delegiertes Security Incident Response-Administratorkonto in einem Konto zu. Die Einrichtung ist zwar regional, AWS Security Incident Response bietet aber eine unternehmensweite Abdeckung aller unterstützten Bereiche. AWS-Regionen Die Sicherheitsergebnisse stammen von Amazon GuardDuty und AWS Security Hub CSPM werden aus allen unterstützten Fällen übernommen AWS-Regionen, und alle Fälle werden zentral in der Region verwaltet, in der Sie Ihr Abonnement aktiviert haben. Das delegierte Security Incident Response-Administratorkonto und die Mitgliedskonten müssen über hinzugefügt werden. AWS Organizations

Es wird nicht empfohlen, das Verwaltungskonto Ihrer Organisation als delegiertes Security Incident Response-Administratorkonto einzurichten.

Das Verwaltungskonto Ihrer Organisation kann das delegierte Security Incident Response-Administratorkonto sein. Die bewährten AWS Sicherheitsmethoden folgen jedoch dem Prinzip der geringsten Rechte und empfehlen diese Konfiguration nicht.

Wenn Sie ein delegiertes Security Incident Response-Administratorkonto aus einem Live-Abonnement entfernen, wird das Abonnement sofort gekündigt.

Wenn Sie ein delegiertes Security Incident Response-Administratorkonto entfernen, werden alle Mitgliedskonten AWS Security Incident Response entfernt, die diesem delegierten Security Incident Response-Administratorkonto zugeordnet sind. AWS Security Incident Response wird nicht mehr für alle Mitgliedskonten aktiviert.

Vertrauenswürdigen Zugriff aktivieren für AWS -Kontenverwaltung

Durch die Aktivierung des vertrauenswürdigen Zugriffs für AWS Security Incident Response kann der delegierte Administrator des Verwaltungskontos die Informationen und Metadaten (z. B. primäre oder alternative Kontaktdaten) für jedes Mitgliedskonto in AWS Organizationsändern.

Gehen Sie wie folgt vor, um vertrauenswürdigen Zugriff für Ihre Organisation AWS Security Incident Response zu aktivieren.

> **Mindestberechtigungen**
>
> Um diese Aufgaben ausführen zu können, müssen Sie die folgenden Anforderungen erfüllen:
>
> - Sie können dies nur über das Verwaltungskonto der Organisation ausführen.
> - Für Ihre Organisation müssen alle Funktionen aktiviert sein.

Console

Um den vertrauenswürdigen Zugriff zu aktivieren für AWS Security Incident Response

1. Melden Sie sich bei der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie im Navigationsbereich Dienste aus.
3. Wählen Sie AWS Security Incident Responsein der Liste der Dienste aus.
4. Wählen Sie Vertrauenswürdigen Zugriff aktivieren.
5. Geben Sie im AWS Security Incident Response Dialogfeld Vertrauenswürdigen Zugriff aktivieren für den Text enable ein, um dies zu bestätigen, und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.

API/CLI

Um vertrauenswürdigen Zugriff zu aktivieren für AWS -Kontenverwaltung

Nachdem Sie den folgenden Befehl ausgeführt haben, können Sie Anmeldeinformationen aus dem Verwaltungskonto der Organisation verwenden, um API-Operationen für die Kontoverwaltung aufzurufen, die den `--accountId` Parameter verwenden, um auf Mitgliedskonten in einer Organisation zu verweisen.

- AWS CLI: enable-aws-service-access

  Im folgenden Beispiel wird der vertrauenswürdige Zugriff für AWS Security Incident Response die Organisation des anrufenden Kontos aktiviert.

```
$ aws organizations enable-aws-service-access \
                                        --service-principal security-
ir.amazonaws.com
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

Für die Benennung eines delegierten Security Incident Response-Administratorkontos sind Berechtigungen erforderlich

Sie können wählen, ob Sie Ihre AWS Security Incident Response Mitgliedschaft mit dem delegierten Administrator für einrichten möchten. AWS Organizations Informationen darüber, wie diese Berechtigungen gewährt werden, finden Sie unter Zusammen AWS Organizations mit anderen AWS Diensten verwenden.

> **Note**
>
> AWS Security Incident Response aktiviert automatisch die AWS Organizations vertrauenswürdige Beziehung, wenn die Konsole für die Einrichtung und Verwaltung verwendet wird. Wenn Sie das verwenden, müssen Sie CLI/SDK dies manuell aktivieren, indem Sie die Enable AWSServiceAccess API verwenden, um zu vertrauen`security-ir.amazonaws.com`.

Stellen Sie als AWS Organizations Manager sicher, dass Sie die folgenden AWS Security Incident Response Aktionen ausführen können, bevor Sie das delegierte Security Incident Response-Administratorkonto für Ihre Organisation festlegen: `security-ir:CreateMembership` und. `security-ir:UpdateMembership` Mit diesen Aktionen können Sie das delegierte Security Incident Response-Administratorkonto für Ihre Organisation festlegen, indem Sie. AWS Security Incident Response Sie müssen außerdem sicherstellen, dass Sie die AWS Organizations Aktionen ausführen dürfen, mit denen Sie Informationen über Ihre Organisation abrufen können.

Um diese Berechtigungen zu gewähren, fügen Sie die folgende Erklärung in eine AWS Identity and Access Management (IAM-) Richtlinie für Ihr Konto ein:

```
        {
            "Sid": "PermissionsForSIRAdmin",
```

```
            "Effect": "Allow",
            "Action": [
                "security-ir:CreateMembership",
                "security-ir:UpdateMembership",
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
```

Wenn Sie Ihr AWS Organizations Verwaltungskonto als delegiertes Security Incident Response-Administratorkonto festlegen möchten, benötigt Ihr Konto auch die IAM-Aktion:. `CreateServiceLinkedRole` Überprüfen Sie diesÜberlegungen und Empfehlungen zur Verwendung mit AWS Security Incident Response AWS Organizations, bevor Sie mit dem Hinzufügen der Berechtigungen fortfahren.

Um mit der Festlegung Ihres AWS Organizations Verwaltungskontos als delegiertes Administratorkonto für Security Incident Response fortzufahren, fügen Sie der IAM-Richtlinie die folgende Erklärung hinzu und *111122223333* ersetzen Sie sie durch die AWS-Konto ID Ihres AWS Organizations Verwaltungskontos:

```
        {
         "Sid": "PermissionsToEnableSecurityIncidentResponse"
         "Effect": "Allow",
         "Action": [
          "iam:CreateServiceLinkedRole"
         ],
         "Resource": "arn:aws:iam::111122223333:role/aws-service-role/security-
ir.amazonaws.com/AWSServiceRoleForSecurityIncidentResponse",
         "Condition": {
          "StringLike": {
           "iam:AWSServiceName": "security-ir.amazonaws.com"
          }
         }
        }
```

Benennen Sie einen delegierten Administrator für AWS Security Incident Response

Dieser Abschnitt enthält Schritte zur Benennung eines delegierten Administrators in der Organisation. AWS Security Incident Response

Stellen Sie als Manager der AWS Organisation sicher, dass Sie sich die Informationen zur Funktionsweise eines delegierten Security Incident Response-Administratorkontos durchlesen. Überlegungen und Empfehlungen Bevor Sie fortfahren, stellen Sie sicher, dass Sie Für die Benennung eines delegierten Security Incident Response-Administratorkontos sind Berechtigungen erforderlich

Wählen Sie eine bevorzugte Zugriffsmethode, um ein delegiertes Security Incident Response-Administratorkonto für Ihr Unternehmen festzulegen. Nur ein Management kann diesen Schritt ausführen.

Console

1. Öffnen Sie die Security Incident Response-Konsole unter https://console.aws.amazon.com/security-ir/

   Um sich anzumelden, verwenden Sie die Verwaltungsdaten Ihrer AWS Organizations Organisation.
2. Wählen Sie mithilfe der AWS-Region Auswahltaste in der oberen rechten Ecke der Seite die Region aus, in der Sie das delegierte Security Incident Response-Administratorkonto für Ihr Unternehmen einrichten möchten.
3. Folgen Sie dem Einrichtungsassistenten, um Ihre Mitgliedschaft einschließlich des delegierten Administratorkontos zu erstellen.

API/CLI

- Führen Sie die Ausführung CreateMembership mit den Anmeldeinformationen AWS-Konto des Managements der Organisation aus.
  - Alternativ können Sie AWS Command Line Interface dies verwenden. Der folgende AWS CLI Befehl bestimmt ein delegiertes Security Incident Response-Administratorkonto.

Im Folgenden sind die Zeichenkettenoptionen aufgeführt, die für die Konfiguration Ihrer Mitgliedschaft verfügbar sind:

```
                                    {
                                      "customerAccountId": "stringstring",
                                      "membershipName": "stringstring",
                                      "customerType": "Standalone",
                                      "organizationMetadata": {
                                        "organizationId": "string",
                                        "managementAccountId":
"stringstring",
                                        "delegatedAdministrators": [
                                          "stringstring"
                                        ]
                                      },
                                      "membershipAccountsConfigurations":
{
                                        "autoEnableAllAccounts": true,
                                        "organizationalUnits": [
                                          "string"
                                        ]
                                      },
                                      "incidentResponseTeam": [
                                        {
                                          "name": "string",
                                          "jobTitle": "stringstring",
                                          "email": "stringstring"
                                        }
                                      ],
                                      "internalIdentifier": "string",
                                      "membershipId": "stringstring",
                                      "optInFeatures": [
                                        {
                                          "featureName": "RuleForwarding",
                                          "isEnabled": true
                                        }
                                      ]
                                    }
```

Wenn AWS Security Incident Response es für Ihr delegiertes Security Incident Response-Administratorkonto nicht aktiviert ist, kann es keine Aktion ausführen. Falls dies noch nicht

geschehen ist, stellen Sie sicher, dass Sie die Aktivierung AWS Security Incident Response für das neu benannte delegierte Security Incident Response-Administratorkonto vornehmen.

Verwaltung der Mitgliedschaft bei Organisationseinheiten (OUs) für AWS Security Incident Response

AWS Security Incident Response unterstützt den Mitgliederschutz für einzelne Organisationseinheiten (OUs). Sie können Ihre Mitgliedschaft OUs jederzeit auf bestimmte Bereiche aktualisieren. Alle Konten innerhalb der ausgewählten OUs Kategorie, einschließlich Konten für Kinder OUs, fallen unter Ihre Mitgliedschaft.

Bei der Aktualisierung Ihres Mitgliedsverbands können Aktualisierungen für bis zu 5 Personen OUs gleichzeitig vorgenommen werden. Wenn Sie Änderungen an mehr als 5 vornehmen möchten OUs, führen Sie die Zuordnungsänderungen in Stapeln von 5 durch, OUs bis alle Aktualisierungen abgeschlossen sind.

Console

1. Öffnen Sie die Security Incident Response-Konsole unter https://console.aws.amazon.com/security-ir/

   Um sich anzumelden, verwenden Sie die Verwaltungsdaten Ihrer AWS Organizations Organisation.
2. Navigieren Sie zu Mitgliedschaft verwalten > Konten
3. Klicken Sie auf Zuordnung aktualisieren
4. Wählen Sie Organisationseinheiten auswählen (OUs)
5. Wählen Sie Hinzufügen OUs oder Entfernen OUs
6. Wählen Sie bis zu 5 aus, die OUs Sie aktualisieren möchten. Sie können nicht gleichzeitig hinzufügen und entfernen OUs .

   > **Note**
   >
   > Alle Konten und Kinder OUs unter einer ausgewählten Organisationseinheit werden verknüpft.
7. Klicken Sie auf Zuordnung aktualisieren

8.

> **Note**
>
> Wenn Sie Änderungen an mehr als 5 vornehmen möchten OUs, wiederholen Sie die Schritte 5 und 6, bis alle verknüpft OUs sind.

Weitere Informationen darüber, wie Sie Änderungen an der Organisationseinheit innerhalb Ihrer AWS Organisation vornehmen können, finden Sie unter Organisationseinheiten verwalten (OUs) mit AWS Organizations.

Mitglieder hinzufügen zu AWS Security Incident Response

Es besteht eine Eins-zu-Eins-Beziehung mit AWS Organizations und Ihrer AWS Security Incident Response Mitgliedschaft. Wenn Konten zu Ihren Organizations oder Organisationseinheiten () hinzugefügt (oder entferntOUs) werden, werden diese Änderungen in den betroffenen Konten für Ihre AWS Security Incident Response Mitgliedschaft berücksichtigt.

Um Ihrer Mitgliedschaft ein Konto hinzuzufügen, folgen Sie einer der Optionen zur Verwaltung von Konten in einer Organisation mit AWS Organizations.

Sie können Ihrer Mitgliedschaft auch jederzeit weitere OUs hinzufügen — siehe Mitgliedschaft mit Organisationseinheiten verwalten (OUs).

Mitglieder entfernen von AWS Security Incident Response

Um ein Konto aus Ihrer Mitgliedschaft zu entfernen, können Sie ein Mitgliedskonto aus Ihrer Organisation entfernen, Konten aus Ihren ausgewählten OUs Konten entfernen oder OUs aus Ihrer Mitgliedschaft entfernen.

Um ein Konto aus Ihrer Mitgliedschaft zu entfernen, folgen Sie den Anweisungen zum Entfernen eines Mitgliedskontos aus einer Organisation.

Um Konten aus Ihrem Konto zu verschieben OUs, folgen Sie den Anweisungen für das Verschieben von Konten in eine Organisationseinheit (OU) oder zwischen Stamm- und OUs With-Konten AWS Organizations.

Um eine Organisationseinheit aus Ihrer Mitgliedschaft zu entfernen, folgen Sie den Anweisungen unter Mitgliedschaft mit Organisationseinheiten verwalten (OUs).

Amazon EventBridge

Mit Amazon EventBridge können Sie auf Ereignisse im Zusammenhang mit AWS Security Incident Response Fällen und Mitgliedschaften reagieren, diese überwachen und orchestrieren. Sie können diese Ereignisse entweder über Regeln (für Fanout-Szenarien an ein oder mehrere Ziele) oder über Pipes (für point-to-point Integrationen mit erweiterten Filter-, Anreicherungs- und Transformationsfunktionen) weiterleiten.

Sie können Integrationen zwischen Security Incident Response und Tools von Drittanbietern erstellen oder Daten aggregieren, um sie mit generativer KI und anderen Tools zu analysieren. AWS Wenn Security Incident Response beispielsweise proaktiv einen Fall erstellt, können Sie mithilfe von EventBridge Automatisierungen Systeme auslösen, die die Beteiligten benachrichtigen. Wenn Sie mehrere AWS Umgebungen verwalten, können Sie außerdem die EventBridge Amazon-Integration verwenden, um AWS Security Incident Response Mitgliedschaften zu überwachen, um sicherzustellen, dass alle Umgebungen ein hohes Maß an Sicherheit gewährleisten.

Weitere Informationen finden Sie unter Was ist Amazon EventBridge?

> **Note**
>
> Die neuesten Updates zur EventBridge Amazon-Integration mit AWS Security Incident Response, einschließlich ITSM-Integrationen, finden Sie unter AWS Security Incident Response unterstützt jetzt ITSM-Integrationen auf der Seite AWS Was ist neu.

Inhalt

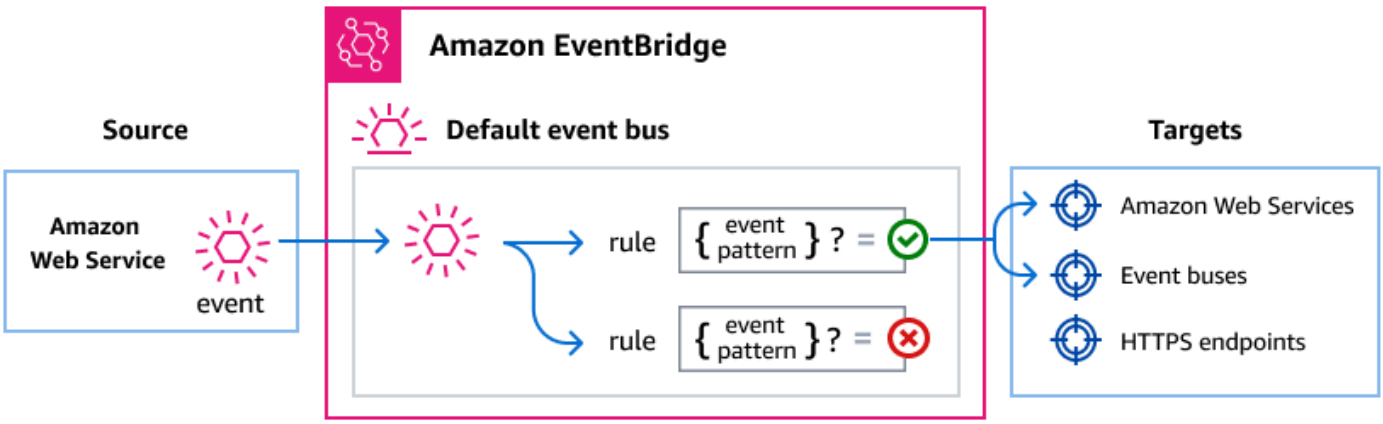
Verwaltung von Ereignissen zur Reaktion auf Sicherheitsvorfälle mithilfe von Amazon EventBridge

Amazon EventBridge ist ein serverloser Service, der Ereignisse verwendet, um Anwendungskomponenten miteinander zu verbinden, sodass Sie leichter skalierbare,

ereignisgesteuerte Anwendungen erstellen können. Bei der ereignisgesteuerten Architektur werden lose gekoppelte Softwaresysteme entwickelt, die zusammenarbeiten, indem sie Ereignisse senden und darauf reagieren. Ereignisse stellen eine Veränderung in einer Ressource oder Umgebung dar.

Funktionsweise:

Wie bei vielen AWS Services generiert Security Incident Response Ereignisse und sendet sie an den EventBridge Standard-Event-Bus. (Der Standard-Event-Bus wird automatisch in Ihrem AWS Konto bereitgestellt.) Ein Event Bus ist ein Router, der Ereignisse empfängt und sie an null oder mehr Ziele weiterleitet. Die Regeln, die Sie für den Event Bus festlegen, werten die Ereignisse aus, sobald sie eintreffen. Jede Regel prüft, ob ein Ereignis dem Ereignismuster der Regelentspricht. Wenn das Ereignis übereinstimmt, sendet der Event Bus das Ereignis an das/die angegebene(n) Ziel(e).



Bereitstellen von Ereignissen zur Reaktion auf Sicherheitsvorfälle mithilfe von EventBridge Regeln

Damit der EventBridge Standardereignisbus Security Incident Response-Ereignisse an ein Ziel sendet, müssen Sie eine Regel erstellen. Jede Regel enthält ein Ereignismuster, das EventBridge mit jedem Ereignis übereinstimmt, das auf dem Event-Bus empfangen wurde. Wenn die Ereignisdaten mit dem angegebenen Ereignismuster EventBridge übereinstimmen, wird dieses Ereignis an die Ziele der Regel gesendet.

Umfassende Anweisungen zur Erstellung von Event-Bus-Regeln finden Sie im EventBridge Amazon-Benutzerhandbuch unter Regeln erstellen, die auf Ereignisse reagieren.

Erstellen eines Ereignismusters, das den Ereignissen von Security Incident Response entspricht

Jedes Ereignismuster ist ein JSON-Objekt, das Folgendes enthält:

- Ein `source`-Attribut, das den Service identifiziert, der das Ereignis sendet. Für Ereignisse im Zusammenhang mit der Reaktion auf Sicherheitsvorfälle lautet die Quelle`"aws.security-ir"`.
- (Optional): Ein `detail-type`-Attribut, das ein Array der zuzuordnenden Ereignistypen enthält.
- (Optional): Ein `detail`-Attribut, das alle anderen Ereignisdaten für den Abgleich enthält.

Das folgende Ereignismuster entspricht beispielsweise allen `Case Updated by AWS Security Incident Response Service` Ereignissen für ein bestimmtes Ereignis AWS-Konto:

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T03:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

Weitere Informationen zum Schreiben von Ereignismustern finden Sie unter Ereignismuster im EventBridge Benutzerhandbuch.

Detaillierte Referenz zu Ereignissen im Bereich Security Incident Response

Alle Ereignisse von AWS Diensten haben einen gemeinsamen Satz von Feldern, die Metadaten über das Ereignis enthalten, z. B. den AWS Dienst, der die Quelle des Ereignisses darstellt, den Zeitpunkt, zu dem das Ereignis generiert wurde, das Konto und die Region, in der das Ereignis

stattgefunden hat, und andere. Definitionen dieser allgemeinen Felder finden Sie unter Referenz zur Ereignisstruktur im EventBridge Amazon-Benutzerhandbuch.

Darüber hinaus weist jedes Ereignis ein `detail`-Feld auf, das spezifische Daten für das betreffende Ereignis enthält. In der folgenden Referenz werden die Detailfelder für die verschiedenen Ereignisse zur Reaktion auf Sicherheitsvorfälle definiert.

Bei der EventBridge Auswahl und Verwaltung von Security Incident Response-Ereignissen ist es hilfreich, Folgendes zu beachten:

- Das `source` Feld für alle Ereignisse aus Security Incident Response ist auf gesetzt`"aws.security-ir"`.
- Das Feld `detail-type` gibt den Ereignistyp an.

  Beispiel, `"Case Updated"`.
- Das Feld `detail` enthält die Daten, die für das betreffende Ereignis spezifisch sind.

Informationen zur Erstellung von Ereignismustern, mit denen Regeln den Ereignissen der Reaktion auf Sicherheitsvorfälle entsprechen, finden Sie unter Ereignismuster im EventBridge Amazon-Benutzerhandbuch.

Weitere Informationen zu Ereignissen und deren EventBridge Verarbeitung finden Sie unter EventBridge Ereignisse im EventBridge Amazon-Benutzerhandbuch.

Allgemeine Felder: Alle AWS Security Incident Response Ereignisse enthalten diese EventBridge Amazon-Standardfelder

- Version: Version im EventBridge Ereignisformat
- id: Eindeutiger Bezeichner für das Ereignis
- detail-type: Für Menschen lesbare Beschreibung des Ereignistyps
- Quelle: Immer „aws.security-ir“ für Security Incident Response-Ereignisse
- AWS Konto: Konto-ID, unter der das Ereignis eingetreten ist
- Zeit: ISO 8601-Zeitstempel, zu dem das Ereignis eingetreten ist
- Region: AWS-Region wo die Ressource existiert
- resources: Array, das den ARN der betroffenen Ressource enthält

Detailfelder: Das `detail` Objekt enthält spezifische Informationen zur Reaktion auf Sicherheitsvorfälle

- CaseID: Eindeutige Kennung für den Fall (nur Fallereignisse)
- membershipId: Eindeutige Kennung für die Mitgliedschaft (nur Mitgliedschaftsveranstaltungen)
- updatedBy: Wer hat die Aktualisierung durchgeführt (nur Ereignisse zur Aktualisierung von Fällen und Kommentaren)
- createdBy: Wer hat die Entität erstellt (nur Ereignisse bei der Erstellung von Fällen und Kommentaren)

Akteurwerte: Die `createdBy` Felder `updatedBy` und können Folgendes enthalten

- AWS Responder: Aktion, die von einem AWS Sicherheits-Responder ausgeführt wurde
- *`security-ir.amazonaws.com`*: Aktion, die automatisch vom Dienst ausgeführt wird
- Konto-ID: Vom Kunden ausgeführte Aktion (z. B. „111122223333“)

ARN-Werte für AWS Security Incident Response Ressourcen: Ressourcen verwenden diese ARN-Formate

- Fälle: `arn:aws:security-ir:{region}:{account-id}:case/{case-id}`
- Mitgliedschaften: `arn:aws:security-ir:{region}:{account-id}:membership/{membership-id}`

Fallereignisse

Von AWS Responder erstellter Fall

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
```

```
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "AWS Responder"
  }
}
```

Vom Service erstellter Fall

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "security-ir.amazonaws.com"
  }
}
```

Vom Kunden erstellter Fall

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
```

```
  "detail": {
    "caseId": "1234567890",
    "createdBy": "111122223333"
  }
}
```

Fall wurde von AWS Responder aktualisiert

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T01:30:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "AWS Responder"
  }
}
```

Fall wurde vom AWS Kunden aktualisiert

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
```

```
    "caseId": "1234567890",
    "updatedBy": "111122223333"
  }
}
```

Fall wurde vom AWS Security Incident Response Service aktualisiert

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T03:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

Fall abgeschlossen

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Closed",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-15T14:22:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890"
```

```
  }
}
```

Ereignisse im Fallkommentar

Von AWS Responder erstellter Fallkommentar

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T04:30:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "AWS Responder"
  }
}
```

Vom Kunden erstellter Fallkommentar

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
```

```
    "createdBy": "111122223333"
  }
}
```

Vom AWS Security Incident Response Service erstellter Fallkommentar

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "security-ir.amazonaws.com"
  }
}
```

Fallkommentar wurde vom Kunden aktualisiert

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "111122223333"
```

```
  }
}
```

Fallkommentar wurde vom AWS Security Incident Response Service aktualisiert

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

Von AWS Responder erstellter Fallkommentar

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "AWS Responder"
  }
```

```
            }
```

Veranstaltungen zur Mitgliedschaft

Mitgliedschaft wurde erstellt

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Created",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-04-01T10:00:00Z",
              "region": "us-west-2",
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

Mitgliedschaft aktualisiert

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Updated",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-04-15T16:30:00Z",
              "region": "us-west-2",
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
```

```
    }
  }
```

Mitgliedschaft gekündigt

```
  {
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Membership Closed",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-06-30T23:59:59Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
    ],
    "detail": {
      "membershipId": "m-1234567890abcdef0"
    }
  }
```

Mitgliedschaft beendet

```
  {
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Membership Terminated",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-07-01T00:00:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:membership/
m-123456s7890abcdef0"
    ],
    "detail": {
      "membershipId": "m-1234567890abcdef0"
    }
```

```
    }
```

AWS Security Incident Response Ereignisse verwenden

Sie können EventBridge Regeln erstellen, die diesen Ereignissen entsprechen und automatisierte Aktionen auslösen. Nachfolgend sind einige beispielhafte Anwendungsfälle aufgeführt:

Alle AWS Security Incident Response Ereignisse zuordnen:

```
{
  "source": ["aws.security-ir"]
}
```

Nur Ereignisse mit Groß- und Kleinschreibung abgleichen:

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
    "Case Comment Added",
    "Case Comment Updated"
  ]
}
```

Von AWS Responders aktualisierte Fälle zuordnen:

```
{
  "source": ["aws.security-ir"],
  "detail-type": ["Case Updated"],
  "detail": {
    "updatedBy": ["AWS Responder"]
  }
}
```

Ereignisse für einen bestimmten Fall zuordnen:

```
{
  "source": ["aws.security-ir"],
  "detail": {
    "caseId": ["1234567890"]
  }
}
```

Tutorial: Senden von Amazon Simple Notification Service-Benachrichtigungen für **`Membership Updated`** Ereignisse

In diesem Tutorial konfigurieren Sie eine EventBridge Amazon-Ereignisregel, die nur Ereignisse erfasst, bei denen Ihr Abonnement einen `Membership Updated` Status annimmt.

Voraussetzungen

In diesem Tutorial wird davon ausgegangen, dass Sie ein funktionierendes Abonnement und aktive AWS Konten in Ihrer Mitgliedschaft haben.

Themen

- Tutorial: Ein Amazon SNS SNS-Thema erstellen und abonnieren
- Tutorial: Registrieren Sie eine Ereignisregel
- Tutorial: Testen Sie Ihre Regel
- Alternative Regel: Fallaktualisierungen zur Reaktion auf Sicherheitsvorfälle

Tutorial: Ein Amazon SNS SNS-Thema erstellen und abonnieren

Mit diesem Tutorial konfigurieren Sie ein Amazon SNS-Thema, das als Ereignisziel für Ihre neue Ereignisregel dient.

Erstellen eines Amazon SNS-Themas

1. Öffnen Sie die Amazon SNS SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie Themen, Thema erstellen aus.
3. Wählen Sie unter Type (Typ) die Option Standard aus.

4. Geben Sie als Namen Thema ein **`MembershipUpdated`** und wählen Sie Create topic aus.
5. Wählen Sie auf dem MembershipUpdatedBildschirm die Option Abonnement erstellen aus.
6. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus.
7. Geben Sie für Endpunkt eine E-Mail-Adresse ein, auf die Sie aktuell Zugriff haben, und wählen Sie Abonnement erstellen aus.
8. Überprüfen Sie Ihr E-Mail-Konto und warten Sie auf eine E-Mail-Nachricht zur Bestätigung Ihres Abonnements. Wenn Sie sie erhalten, wählen Sie Confirm Abonnement aus.

Tutorial: Registrieren Sie eine Ereignisregel

Als Nächstes registrieren Sie eine Ereignisregel, die nur `Membership Updated` Ereignisse erfasst.

Um Ihre EventBridge Regel zu registrieren

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

   > **Note**
   >
   > Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.

5. Wählen Sie als Event bus (Event Bus) den Event Bus aus, den Sie dieser Regel zuordnen möchten. Wenn Sie möchten, dass diese Regel mit Ereignissen aus Ihrem eigenen Konto übereinstimmt, wählen Sie AWS -Standard-Event-Bus aus. Wenn ein AWS Service in Ihrem Konto ein Ereignis ausgibt, wird dieses immer an den Standard-Event-Bus Ihres Kontos weitergeleitet.

   > **Note**
   >
   > Dies sollte in Ihrem AWS Organizations oder einem delegierten Administratorkonto eingerichtet werden, in dem Sie die AWS Security Incident Response Mitgliedschaft erstellt haben.

6. Bei Regeltyp wählen Sie Regel mit einem Ereignismuster aus.

7. Wählen Sie Weiter aus.
8. Wählen Sie für Event source (Ereignisquelle) Other (Andere) aus.
9. Wählen Sie unter Ereignismuster die Option Benutzerdefinierte Muster (JSON-Editor) aus.
10. Fügen Sie das folgende Ereignismuster in das Textfeld ein.

```
{
  "source": ["aws.security-ir"],
  "detail-type": ["Membership Updated"]
}
```

    Dieser Code definiert eine EventBridge Regel, die für jedes Ereignis gilt, bei dem Ihre Dienstmitgliedschaft aktualisiert oder geändert wird. Weitere Informationen zu Ereignismustern finden Sie unter Ereignisse und Ereignismuster im EventBridge Amazon-Benutzerhandbuch.
11. Wählen Sie Weiter aus.
12. Bei Zieltypen wählen Sie AWS -Service aus.
13. Wählen Sie für Wählen Sie ein Ziel die Option SNS-Thema und für Thema die Option MembershipUpdated.
14. (Optional) Gehen Sie unter Additional settings (Weitere Einstellungen) wie folgt vor:

    a. Geben Sie für Maximum age of event (Maximales Alter des Ereignisses) einen Wert zwischen einer Minute (00:01) und 24 Stunden (24:00) ein.

    b. Geben Sie für Wiederholungsversuche eine Zahl zwischen 0 und 185 ein.

    c. Wählen Sie für Warteschlange für unzustellbare Briefe aus, ob Sie eine standardmäßige Amazon SQS SQS-Warteschlange als Warteschlange für unzustellbare Briefe verwenden möchten. EventBridge sendet Ereignisse, die dieser Regel entsprechen, an die Warteschlange für unzustellbare Briefe, wenn sie nicht erfolgreich an das Ziel zugestellt wurden. Führen Sie eine der folgenden Aktionen aus:

        - Klicken Sie auf Keine, um keine Warteschlange für unzustellbare Nachrichten zu verwenden.
        - Wählen Sie Wählen Sie eine Amazon SQS SQS-Warteschlange im aktuellen AWS Konto aus, die als Warteschlange für eingehende Briefe verwendet werden soll, und wählen Sie dann die zu verwendende Warteschlange aus der Drop-down-Liste aus.
        - Wählen Sie Wählen Sie eine Amazon SQS SQS-Warteschlange in einem anderen AWS Konto als Warteschlange für unzustellbare Briefe aus und geben Sie dann den ARN

der Warteschlange ein, die Sie verwenden möchten. Sie müssen der Warteschlange eine ressourcenbasierte Richtlinie beifügen, die das Senden von Nachrichten an die EventBridge Warteschlange ermöglicht. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch unter Erteilen von Berechtigungen für die Warteschlange mit unzustellbaren Briefen.

15. Wählen Sie Weiter aus.
16. (Optional) Geben Sie ein oder mehrere Tags für die Regel ein. Weitere Informationen finden Sie unter EventBridge Amazon-Tags im EventBridge Amazon-Benutzerhandbuch.
17. Wählen Sie Weiter aus.
18. Überprüfen Sie die Details der Regel und wählen Sie dann Regel erstellen aus.

Tutorial: Testen Sie Ihre Regel

Um deine Regel zu testen, reiche ein Update zu deiner AWS Security Incident Response Mitgliedschaft ein. Wenn Ihre Regel korrekt konfiguriert ist, sollten Sie innerhalb weniger Minuten eine E-Mail-Nachricht mit dem Ereignistext erhalten.

Alternative Regel: Fallaktualisierungen zur Reaktion auf Sicherheitsvorfälle

Um eine Ereignisregel zu erstellen, die alle Fallaktualisierungen überwacht, wiederholen Sie diese Tutorials mit den folgenden Änderungen:

1. In Tutorial: Ein Amazon SNS SNS-Thema erstellen und abonnieren, *CaseUpdates* als Themennamen verwenden.
2. Verwenden Sie in Tutorial: Registrieren Sie eine Ereignisregel das folgende Muster im JSON-Editor:

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
    "Case Comment Created",
    "Case Comment Updated"
  ]
}
```

Fehlerbehebung

Wenn Sie Probleme im Zusammenhang mit der Durchführung einer bestimmten Aktion für haben AWS Security Incident Response, lesen Sie die Themen in diesem Abschnitt.

Ein FEHLER ist ein Status eines Vorgangs, der auf einen Fehler bei einigen oder allen Vorgängen hinweist. Alternativ erhalten Sie Warnungen, wenn ein Problem auftritt, die Aufgabe aber trotzdem abgeschlossen ist.

Inhalt

Problembereiche

Anfragen werden nicht aus dem richtigen Kontext gesendet.

Alle Aufrufe an AWS Security Incident Response APIs müssen von einem IAM-Prinzipal im delegierten Administrator- oder Mitgliedskonto des Dienstes stammen. Stellen Sie sicher, dass Sie mit dem richtigen IAM-Prinzipal in dem AWS-Konto AWS Security Incident Response delegierten Administrator- oder Mitgliedskonto Ihrer Organisation arbeiten.

Fehler

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

Bitte arbeiten Sie mit Ihrem AWS Administrator zusammen, um sicherzustellen, dass Sie in Ihrem AWS Security Incident Response delegierten Administrator- oder Mitgliedskonto berechtigt sind, eine IAM-Rolle zu übernehmen. Vergewissern Sie sich auch, dass für die Rolle eine IAM-Richtlinie gilt, die die angeforderte Aktion zulässt. Weitere Informationen finden Sie unter AWS Security Incident Response IAM.

ConflictException

Die Anfrage verursacht einen inkonsistenten Status.

Bitte überprüfen Sie in jedem Fall, ob die von Ihnen angegebenen Namen der Anhangsdateien oder der Mitglieder des Standard-Antwortteams eindeutig sind. Vergewissern Sie sich auch, dass Ihre AWS Security Incident Response Dienstmitgliedschaft nicht bereits konfiguriert wurde. Öffnen Sie die Security Incident Response-Konsole unter https://console.aws.amazon.com/security-ir/ und navigieren Sie zu`Membership Details`.

InternalServerException

Bei der Bearbeitung der Anfrage ist ein unerwarteter Fehler aufgetreten. Bitte versuchen Sie es in ein paar Minuten erneut. Wenn das Problem weiterhin besteht, melden Sie einen Fall bei Support.

ResourceNotFoundException

Die Anfrage verweist auf eine Ressource, die nicht existiert.

Eine oder mehrere der in Ihrer Anfrage angegebenen Ressourcen sind nicht vorhanden. Bitte überprüfen Sie, ob alle angegebenen Ressourcen korrekt IDs sind ARNs oder ob sie korrekt sind. Dies gilt für Konten AWS Organizations IDs IDs, IAM-Rollen, Mitgliedschaften, Fälle, Mitglieder des Reaktionsteams, Fälle, Fallbeantworter, Fallanhänge und Fallkommentare.

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

Ihr IAM-Principal hat in einem bestimmten Zeitraum zu viele Anfragen an diese API-Funktion gestellt. Warten Sie eine Minute und versuchen Sie es erneut. Wenn das Problem weiterhin besteht, erwägen Sie bitte die Implementierung eines Algorithmus für exponentielle Backoffs und Wiederholungen.

ValidationException

Die Eingabe erfüllt nicht die mit einem angegebenen Einschränkungen. AWS-Service

Eines oder mehrere der Datenfelder in Ihrer Anfrage erfüllten nicht die Anforderungen für die and/or logische Kombination der Validierung. Bitte überprüfen Sie, ob alle Ressourcen ARNs vollständig sind und ob die Textwerte die Größen- und Formatbeschränkungen aus dem AWS Security Incident Response API-Referenzhandbuch erfüllen. Vergewissern Sie sich auch, dass Wertaktualisierungen zulässig sind. Es ist beispielsweise nicht möglich, einen Fall von „ AWS unterstützt“ in „Selbstverwaltet“ zu ändern.

Support

Wenn Sie zusätzliche Unterstützung benötigen, wenden Sie sich zur Problembehebung an das Support Center. Halten Sie bitte die folgenden Informationen bereit:

- Die AWS-Region , die du benutzt hast
- Die AWS-Konto ID der Mitgliedschaft
- Ihr Quellinhalt, falls zutreffend und verfügbar
- Alle weiteren Details zu dem Problem, die bei der Problembehebung hilfreich sein könnten

Sicherheit

Inhalt

Datenschutz in AWS Security Incident Response

Inhalt

Das Modell der AWS gemeinsamen Verantwortung gilt für den Datenschutz für den AWS Security Incident Response Service. AWS Ist, wie in diesem Modell beschrieben, für den Schutz der Infrastruktur verantwortlich, auf der die in der AWS Cloud angebotenen Dienste ausgeführt werden. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben der von Ihnen verwendeten AWS Dienste 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 die GDPRAWS im Blog zur -Sicherheit.

Aus Datenschutzgründen besagen bewährte AWS Sicherheitsmethoden, dass Sie die AWS Kontoanmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten sollten. Auf diese Weise erhält jeder Benutzer nur die Berechtigungen, die zur Erfüllung seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. 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 Standardsicherheitskontrollen innerhalb der AWS Dienste.
- FIPS 140-3 wird derzeit vom Dienst nicht unterstützt.

Sie sollten niemals vertrauliche oder sensible Informationen wie Ihre E-Mail-Adressen in Tags oder frei formatierte Textfelder wie ein Namensfeld eingeben. Dies gilt auch, wenn Sie mit AWS Support oder anderen AWS Diensten über die Konsole, API, AWS CLI oder arbeiten AWS SDKs. Alle Daten, die Sie in Tags oder Freiform-Textfelder für Namen eingeben, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server angeben, empfehlen wir dringend, dass Sie in der URL keine Anmeldeinformationen angeben, um Ihre Anfrage an diesen Server zu überprüfen.

Datenverschlüsselung

Inhalt

Verschlüsselung im Ruhezustand

Daten werden im Ruhezustand mittels transparenter serverseitiger Verschlüsselung verschlüsselt. Dieser Service reduziert den Ausführungsaufwand und die Komplexität, die mit dem Schutz sensibler Daten verbunden sind. Mit der Verschlüsselung von Daten im Ruhezustand können Sie sicherheitsrelevante Anwendungen erstellen, die Verschlüsselungsvorschriften und gesetzliche Bestimmungen einhalten.

Verschlüsselung während der Übertragung

Daten, die gesammelt und abgerufen werden, erfolgen ausschließlich über einen durch AWS Security Incident Response Transport Layer Security (TLS) geschützten Kanal.

Schlüsselverwaltung

AWS Security Incident Response implementiert Integrationen AWS KMS , um die Verschlüsselung von Fall- und Anhangsdaten im Ruhezustand zu gewährleisten.

AWS Security Incident Response unterstützt keine vom Kunden verwalteten Schlüssel.

Datenschutz für den Datenverkehr zwischen Netzwerken

Datenverkehr zwischen Service und On-Premises-Clients und -Anwendungen

Sie haben zwei Verbindungsoptionen zwischen Ihrem privaten Netzwerk und AWS:

- Eine AWS Site-to-Site VPN Verbindung. Weitere Informationen finden Sie unter Was ist AWS Site-to-Site VPN? im AWS Site-to-Site VPN -Benutzerhandbuch.
- Eine Direct Connect Verbindung. Weitere Informationen finden Sie unter Was ist Direct Connect? im Direct Connect -Benutzerhandbuch.

Der Zugriff AWS Security Incident Response über das Netzwerk erfolgt über eine AWS veröffentlichte Version APIs. Clients müssen Transport Layer Security (TLS) 1.2 unterstützen. Wir empfehlen TLS 1.3. Clients müssen außerdem Cipher Suites mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi. Außerdem müssen Sie die Anfragen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signieren, die einem IAM-Prinzipal zugeordnet sind. Sie können auch AWS -Security-Token-Service (STS) verwenden um temporäre Sicherheitsanmeldeinformationen zu generieren.

Verkehr zwischen AWS Ressourcen in derselben Region

Ein Amazon Virtual Private Cloud (Amazon VPC) -Endpunkt für AWS Security Incident Response ist eine logische Einheit innerhalb einer VPC, die nur Konnektivität für ermöglicht. AWS Security Incident Response Die Amazon VPC leitet Anfragen an die VPC weiter AWS Security Incident Response und

leitet Antworten zurück an diese. Weitere Informationen finden Sie unter VPC-Endpunkte im Amazon-VPC-Benutzerhandbuch. Dieser Abschnitt enthält Beispiele für Richtlinien, die für die Steuerung des Zugriffs auf VPC-Endpunkte verwendet werden können. Sehen Sie Verwenden von IAM-Richtlinien zum Steuern des Zugriffs auf DynamoDB.

> **Note**
>
> Amazon VPC-Endpunkte sind nicht über AWS Site-to-Site VPN oder zugänglich. Direct Connect

Identitäts- und Zugriffsverwaltung

AWS Identity and Access Management (IAM) ist ein AWS Dienst, der einem Administrator hilft, den Zugriff auf AWS Ressourcen zu kontrollieren. IAM-Administratoren kontrollieren authentifizierte (angemeldete) und autorisierte (mit Berechtigungen) Prinzipale für die Nutzung von Ressourcen. AWS Security Incident Response IAM ist ein AWS Dienst, den Sie ohne zusätzliche Kosten nutzen können.

Inhalt

Publikum

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in AWS Security Incident Response der Sie tätig sind.

Sicherheitsadministratoren

Diesen Benutzern wird empfohlen, die AWSSecurityIncidentResponseFullAccessverwaltete Richtlinie zu verwenden, um sicherzustellen, dass sie Lese- und Schreibzugriff auf Mitgliedschafts- und Fallressourcen haben.

Fallbeobachter

Diese Personen haben nicht autorisierten Zugang zu allen Fällen, sondern zu Einzelfällen, für die Sie Ihre ausdrückliche Genehmigung erteilen.

Mitglieder des Incident Response Teams

Mitglieder des Teams können sowohl Vollmitgliedschaft als auch Zugang zu Fällen erhalten. Es wird empfohlen, dass nicht alle Personen über verbindliche Maßnahmen zur Mitgliedschaft im Dienst verfügen, sondern dass sie Zugriff auf alle Fälle haben, die über den Dienst erstellt und verwaltet werden. Weitere Informationen finden Sie unter AWS Security Incident Response Verwaltete Richtlinien.

Authentifizierung mit Identitäten

Bei der Authentifizierung melden Sie sich AWS mit Ihren Identitätsdaten an. Sie müssen als Root-Benutzer des AWS Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle authentifiziert (angemeldet AWS) sein.

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 einen Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich bei der AWS Management Console oder dem AWS Zugriffsportal anmelden. Weitere Informationen zur Anmeldung finden Sie unter So melden Sie sich bei Ihrem AWS Konto an im AWS Anmelde-Benutzerhandbuch. AWS

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenen Signieren von Anforderungen finden Sie unter Signieren von AWS -API-Anforderungen im IAM-Benutzerhandbuch.

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-Factor Authentication im AWS IAM Identity Center User Guide und Using Multi-Factor Authentication (MFA) AWS im IAM-Benutzerhandbuch.

AWS Konto (Root-Benutzer)

Wenn Sie ein AWS Konto erstellen, beginnen Sie mit einer einzigen Anmeldeidentität, die vollständigen Zugriff auf alle AWS Dienste und Ressourcen im Konto hat. Diese Identität wird als Root-Benutzer des AWS Kontos bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Verwenden Sie den Root-Benutzer niemals für Ihre täglichen Aufgaben und ergreifen Sie Maßnahmen, um Ihre Root-Benutzeranmeldedaten zu schützen. Verwenden Sie sie nur, um 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.

Föderierte Identität

Es hat sich bewährt, menschlichen Benutzern, einschließlich Benutzern, die Administratorzugriff benötigen, vorzuschreiben, den Verbund mit einem Identitätsanbieter zu verwenden, um mithilfe temporärer Anmeldeinformationen auf AWS Dienste zuzugreifen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter, dem AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe von Anmeldeinformationen, die über eine Identitätsquelle bereitgestellt wurden, auf AWS Dienste zugreift. Wenn föderierte Identitäten auf AWS Konten zugreifen, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für eine zentralisierte Zugriffsverwaltung empfehlen wir die Verwendung von AWS IAM Identity Center. 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 für alle Ihre AWS Konten und 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 in Ihrem AWS Konto, die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM-Benutzer mit langfristigen Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie einen bestimmten Anwendungsfall haben, für den langfristige Anmeldeinformationen bei IAM-Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. 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 spezifiziert. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen erleichtern die Verwaltung von Berechtigungen für große Benutzergruppen. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM-Ressourcen erteilen.

Benutzer sind nicht dasselbe wie 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 AWS Kontos, die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der AWS Management Console übernehmen, 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 AWS Diensten können Sie 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

- Serviceübergreifender Zugriff — Einige AWS Dienste verwenden Funktionen in anderen AWS Diensten. 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.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle in 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 einem Dienst verknüpft ist. AWS Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen werden in Ihrem AWS Konto angezeigt 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 AWS CLI- oder AWS API-Anfragen stellen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen abzurufen. 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.

Wie AWS Security Incident Response funktioniert mit IAM

AWS Identity and Access Management (IAM) ist ein AWS Dienst, der einem Administrator hilft, 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. AWS Security Incident Response IAM ist ein AWS Dienst, den Sie ohne zusätzliche Kosten nutzen können.

IAM-Funktionen, die Sie mit verwenden können AWS Security Incident Response	
IAM-Funktion	Ausrichtung der Dienste
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Schlüssel zu den politischen Bedingungen	Ja (global)
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Inhalt

Identitätsbasierte Richtlinien für AWS Security Incident Response

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.

Inhalt

Beispiele für identitätsbasierte Richtlinien

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Ressourcen zu erstellen oder zu ändern AWS Security Incident Response . Sie können auch keine Aufgaben mithilfe der AWS Managementkonsole, der AWS Befehlszeilenschnittstelle (AWS CLI) oder der AWS API ausführen. Ein IAM-Administrator kann IAM-Richtlinien erstellen, um Benutzern die Erlaubnis zu erteilen, Aktionen mit den benötigten Ressourcen durchzuführen. 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 den von AWS Security Incident Response definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Security Incident Response in der Service Authorization Reference.

Best Practices für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS Security Incident Response Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Diese Aktionen können mit Kosten für Ihr Konto verbunden sein. AWS Beachten Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Richtlinien und Empfehlungen:

Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem AWS -Konto verfügbar. 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 Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.

Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.

Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten AWS Dienst verwendet werden, 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.

Anforderung einer Multi-Faktor-Authentifizierung (MFA) – Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS -Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der AWS Security Incident Response Konsole

Für den Zugriff https://console.aws.amazon.com/security-ir/ benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS Security Incident Response Ressourcen in Ihrem AWS Konto aufzulisten und einzusehen. 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 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.

Fügen Sie die AWS Security Incident Response Zugriffsrichtlinie oder die ReadOnly AWS verwaltete Richtlinie an, um sicherzustellen, dass Benutzer und Rollen die Servicekonsole verwenden können. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

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 AWS CLI oder AWS API.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien im Rahmen von Security Incident Response AWS

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. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS -Services umfassen.

Weitere Informationen finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen

Politische Maßnahmen für AWS Security Incident Response

Politische Maßnahmen Support: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Action-Element einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Eine Liste der AWS Security Incident Response Aktionen finden Sie unter Aktionen definiert von AWS Security Incident Response in der Serviceautorisierungsreferenz.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS Security Incident Response verwendet:

AWS Security Incident Response -Identität

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

„Aktion“: ["AWS Security Incident Response -identity:Aktion1"," -identity:Aktion2"]AWS Security Incident Response

Richtlinienressourcen für Amazon AWS Security Incident Response

Unterstützt Richtlinienressourcen: Ja, Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement Resource gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder eine Ressource 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": "*"

Schlüssel zur Richtlinienbedingung für AWS Security Incident Response

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Nein

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Mit dem Condition-Element (oder dem Condition-Block) können Sie Bedingungen angeben, unter denen eine Anweisung gültig ist. Das Bedingungselement 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 einzigen Condition-Element angeben, werden diese mithilfe einer logischen UND-Operation AWS ausgewertet. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen OR-Operation aus. Alle Bedingungen müssen erfüllt sein, bevor die Berechtigungen für die Anweisung erteilt 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.

Zugriffskontrolllisten (ACLs) in AWS Security Incident Response

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Attributbasierte Zugriffskontrolle (ABAC) mit Security Incident Response AWS

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und mehrere AWS -Ressourcen anfügen. 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 Taginformationen im Bedingungselement einer Richtlinie mit den Bedingungsschlüsseln AWS: ResourceTag /key-name, AWS: RequestTag /key-name oder: condition ein. AWS TagKeys 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 mit AWS Security Incident Response

Unterstützt temporäre Anmeldeinformationen: Ja

AWS Dienste funktionieren nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich der AWS Dienste, die mit temporären Anmeldeinformationen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren. Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen Methode als

einem Benutzernamen und einem Passwort bei der AWS Management Console anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On (SSO) -Link 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.

Sie können mithilfe der AWS CLI oder AWS API manuell temporäre Anmeldeinformationen 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.

Zugriffssitzungen weiterleiten für AWS Security Incident Response

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 AWS Dienst aufruft, in Kombination mit dem anfordernden AWS Dienst, um Anfragen an nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS Diensten oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

Fehlerbehebung bei AWS Security Incident Response Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Security Incident Response und IAM auftreten können.

Topics

- Ich bin nicht zur Ausführung einer Aktion autorisiert.
- Ich bin nicht berechtigt, IAM durchzuführen: PassRole
- Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine AWS Security Incident Response Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion durchzuführen

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, die Konsole zu verwenden, um Details zu einer fiktiven my-example-widget Ressource anzuzeigen, aber nicht über die fiktiven Berechtigungen für AWS Security Incident Response: verfügt. GetWidget

User: arn ::iam: :123456789012:user/mateojackson ist nicht berechtigt,AWS:: on resource: my - example-widget auszuführen AWS Security Incident Response GetWidget

In diesem Fall muss die Richtlinie für den Benutzer mateojackson aktualisiert werden, um den Zugriff auf die Ressource mithilfe der Aktion: zu ermöglichen. my-example-widget AWS Security Incident Response GetWidget

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 auszuführen: PassRole Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht autorisiert sind, die iam: PassRole -Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an diese Person übergeben können. AWS Security Incident Response

Bei einigen AWS Diensten können Sie eine bestehende Rolle an diesen Dienst 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 namens marymajor versucht, die Konsole zu verwenden, um eine Aktion in AWS Security Incident Response auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

User: arn ::iam: :123456789012:user/marymajor ist nicht berechtigt, Folgendes auszuführen AWS: iam: PassRole

In diesem Fall müssen Marys Richtlinien aktualisiert werden, damit sie die Aktion iam: ausführen kann. PassRole Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine AWS Security Incident Response Ressourcen ermöglichen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Amazon diese Funktionen AWS Security Incident Response unterstützt, finden Sie unter So funktioniert AWS Security Incident Response mit IAM.
- Informationen dazu, wie Sie den Zugriff auf Ihre Ressourcen mit Ihren AWS Konten gewähren können, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS Konto, das Sie besitzen.
- Informationen dazu, wie Sie AWS Konten von Drittanbietern Zugriff auf Ihre Ressourcen gewähren, finden Sie im IAM-Benutzerhandbuch unter Zugriff auf AWS Konten, die Dritten gehören.
- 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwenden von Servicerollen

Unterstützt Servicerollen: Nein

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 im IAM-Benutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen für einen AWS Dienst.

Verwenden von servicegebundenen Rollen

Mit Diensten verknüpfte Rollen für AWS Security Incident Response

Inhalt

- AWS Spiegelreflexkamera: AWSService RoleForSecurityIncidentResponse
- AWS Spiegelreflexkamera: AWSServiceRoleForSecurityIncidentResponse_Triage
- Unterstützte Regionen für serviceverknüpfte Rollen AWS Security Incident Response

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einem AWS Dienst verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS -Konto angezeigt und gehören zum Service. Ein AWS Identity and Access Management Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

Eine dienstverknüpfte Rolle AWS Security Incident Response erleichtert die Einrichtung, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Security Incident Response definiert die Berechtigungen ihrer dienstbezogenen Rollen und AWS Security Incident Response kann, sofern nicht anders definiert, nur ihre Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Informationen zu anderen Diensten, die dienstverknüpfte Rollen unterstützen, finden Sie unter AWS Dienste, die mit IAM funktionieren. Suchen Sie in der Spalte Dienstverknüpfte Rollen nach den Diensten, für die Ja steht. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

AWS Spiegelreflexkamera: AWSService RoleForSecurityIncidentResponse

AWS Security Incident Response verwendet die AWS Security Incident Response SLR-Richtlinie (Service Linked Role), AWSService RoleForSecurityIncidentResponse um abonnierte Konten zu identifizieren, Kundenvorgänge zu erstellen und zugehörige Ressourcen zu kennzeichnen.

Berechtigungen

Die AWSService RoleForSecurityIncidentResponse serviceverknüpfte Rolle vertraut darauf, dass der folgende Dienst die Rolle übernimmt:

- `triage.security-ir.amazonaws.com`

Dieser Rolle ist die AWS verwaltete Richtlinie mit dem Namen zugeordnet. AWSSecurityIncidentResponseServiceRolePolicy Der Dienst verwendet die Rolle, um Aktionen für die folgenden Ressourcen durchzuführen:

- AWS Organizations: Ermöglicht dem Dienst, nach Mitgliedskonten für die Verwendung mit dem Dienst zu suchen.
- CreateCase: Ermöglicht dem Dienst, Servicefälle im Namen von Mitgliedskonten zu erstellen.

- ListCases: Ermöglicht dem KI-Agenten des Dienstes, Fälle für Sicherheitsuntersuchungen einzusehen.
- UpdateCase: Ermöglicht dem KI-Agenten des Dienstes, die Fallmetadaten zu aktualisieren.
- CreateCaseComment: Ermöglicht dem KI-Agenten des Dienstes, seine Ergebnisse als Fallkommentar zu veröffentlichen.
- ListComments: Ermöglicht dem KI-Agenten des Dienstes, Fallkommentare einzusehen, die für die Durchführung automatisierter Untersuchungen erforderlich sind.
- TagResource: Ermöglicht die Service-Tag-Ressourcen, die als Teil des Dienstes konfiguriert wurden.

Die Rolle verwalten

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie AWS Security Incident Response in die AWS-Managementkonsole, die oder die AWS API AWS CLI einsteigen, erstellt der Dienst die mit dem Dienst verknüpfte Rolle für Sie.

> **Note**
>
> Wenn Sie eine Mitgliedschaft mit einem delegierten Administratorkonto erstellt haben, müssen dienstverknüpfte Rollen manuell in AWS Organizations Verwaltungskonten erstellt werden.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie den Dienst in Anspruch nehmen, wird die dienstbezogene Rolle erneut für Sie erstellt.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Berechtigungen für dienstverknüpfte Rollen.

AWS Spiegelreflexkamera: AWSServiceRoleForSecurityIncidentResponse_Triage

AWS Security Incident Response verwendet die sogenannte AWS Security Incident Response SLR-Richtlinie (Service Linked Role), AWSServiceRoleForSecurityIncidentResponse_Triage um

Ihre Umgebung kontinuierlich auf Sicherheitsbedrohungen zu überwachen, Sicherheitsdienste zu optimieren, um Warnmeldungen zu reduzieren, und Informationen zur Untersuchung potenzieller Vorfälle zu sammeln.

Berechtigungen

Die AWSServiceRoleForSecurityIncidentResponse_Triage dienstbezogene Rolle vertraut darauf, dass der folgende Dienst die Rolle übernimmt:

- `triage.security-ir.amazonaws.com`

Dieser Rolle ist die AWS verwaltete Richtlinie zugeordnet. AWSSecurityIncidentResponseTriageServiceRolePolicy Der Dienst verwendet die Rolle, um Aktionen für die folgenden Ressourcen durchzuführen:

- Ereignisse: Ermöglicht dem Dienst, eine Amazon EventBridge verwaltete Regel zu erstellen. Diese Regel ist die Infrastruktur, die in Ihrem AWS Konto erforderlich ist, um Ereignisse von Ihrem Konto an den Dienst zu übertragen. Diese Aktion wird für jede AWS Ressource ausgeführt, die von verwaltet wird`triage.security-ir.amazonaws.com`.
- Amazon GuardDuty: Ermöglicht dem Service, Sicherheitsdienste zu optimieren, um Warngeräusche zu reduzieren, Informationen zur Untersuchung potenzieller Vorfälle zu sammeln und GuardDuty Malware-Scans einzuleiten.
- AWS Security Hub CSPM: Ermöglicht dem Service, aktivierte Standards und Produktintegrationen aufzulisten, Organisationsmitglieder und Administratorkonten aufzulisten und Sicherheitsdienste zu optimieren, um Warnmeldungen zu reduzieren und Informationen zur Untersuchung potenzieller Vorfälle zu sammeln.
- AWS Identity and Access Management: Ermöglicht dem Dienst, Rolleninformationen für die mit dem Dienst `AWSServiceRoleForAmazonGuardDutyMalwareProtection` verknüpfte Rolle abzurufen, um zu überprüfen, ob sie konfiguriert GuardDuty MalwareProtection ist.
- AWS Security Incident Response: Ermöglicht dem Service, Fälle zu erstellen und zu aktualisieren und Ressourcen zu taggen, beschränkt auf Ressourcen, die mit `SecurityIncidentResponseManaged=true` gekennzeichnet sind. Ermöglicht dem Dienst das Lesen von Mitgliedschaftsinformationen (GetMembership, ListMemberships).

Die Rolle verwalten

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie AWS Security Incident Response in die AWS-Managementkonsole, die oder die AWS API AWS CLI einsteigen, erstellt der Dienst die mit dem Dienst verknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie den Service in Anspruch nehmen, wird die dienstbezogene Rolle erneut für Sie erstellt.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Berechtigungen für dienstverknüpfte Rollen.

Unterstützte Regionen für serviceverknüpfte Rollen AWS Security Incident Response

AWS Security Incident Response unterstützt die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen der Service verfügbar ist.

- USA Ost (Ohio)
- USA West (Oregon)
- USA Ost (Virginia)
- Europe (Frankfurt)
- Europa (Irland)
- Europa (London)
- Europa (Milan)
- Europa (Paris)
- Europa (Spain)
- Europa (Stockholm)
- Europa (Zürich)
- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Jakarta)

- Asien-Pazifik (Melbourne)
- Asien-Pazifik (Mumbai)
- Asia Pacific (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Middle East (Bahrain)
- Naher Osten (VAE)
- Südamerika (São Paulo)
- Afrika (Kapstadt)

AWS Verwaltete Richtlinien

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

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 unter AWS Verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS Dienste verwalten und aktualisieren ihre zugehörigen AWS verwalteten Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge 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.

Inhalt

AWS verwaltete Richtlinie: AWSSecurity IncidentResponseServiceRolePolicy

AWS Security Incident Response verwendet die AWSSecurity IncidentResponseServiceRolePolicy AWS verwaltete Richtlinie. Diese AWS verwaltete Richtlinie ist der AWSServiceRoleForSecurityIncidentResponsedienstbezogenen Rolle zugeordnet. Die Richtlinie ermöglicht die Identifizierung abonnierter Konten, das Erstellen von Kundenvorgängen, das Aktualisieren von Kundenvorgängen, das Erstellen von Kundenvorgangskommentaren, das Auflisten von Kundenvorgängen, das Auflisten von Fallkommentaren und das Markieren verwandter Ressourcen. AWS Security Incident Response

> **Important**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen in Tags. AWS Security Incident Response verwendet Tags, um Ihnen Verwaltungsdienste zur Verfügung zu stellen. Tags sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden

Einzelheiten zu den Berechtigungen

Der Dienst verwendet diese Richtlinie, um Aktionen für die folgenden Ressourcen durchzuführen:

- AWS Organizations: Ermöglicht dem Dienst, nach Mitgliedskonten für die Verwendung mit dem Dienst zu suchen.
- CreateCase: Ermöglicht dem Dienst, Servicefälle im Namen von Mitgliedskonten zu erstellen.
- ListCases: Ermöglicht dem KI-Agenten des Dienstes, Fälle für Sicherheitsuntersuchungen einzusehen.
- UpdateCase: Ermöglicht dem KI-Agenten des Dienstes, die Fallmetadaten zu aktualisieren.
- CreateCaseComment: Ermöglicht dem KI-Agenten des Dienstes, seine Ergebnisse als Fallkommentar zu veröffentlichen.
- ListComments: Ermöglicht dem KI-Agenten des Dienstes, Fallkommentare einzusehen, die für die Durchführung automatisierter Untersuchungen erforderlich sind.
- TagResource: Ermöglicht die Service-Tag-Ressourcen, die als Teil des Dienstes konfiguriert wurden.

Sie können die mit dieser Richtlinie verknüpften Berechtigungen unter AWS Verwaltete Richtlinien für einsehen AWSSecurityIncidentResponseServiceRolePolicy.

AWS verwaltete Richtlinie: AWSSecurity IncidentResponseFullAccess

AWS Security Incident Response verwendet die AWSSecurity IncidentResponseAdmin AWS verwaltete Richtlinie. Diese Richtlinie gewährt vollen Zugriff auf Serviceressourcen und Zugriff auf verwandte Ressourcen AWS-Services. Sie können diese Richtlinie zusammen mit Ihren IAM-Prinzipalen verwenden, um schnell Berechtigungen für hinzuzufügen. AWS Security Incident Response

> **Important**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen in Tags. AWS Security Incident Response verwendet Tags, um Ihnen Verwaltungsdienste zur Verfügung zu stellen. Tags sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden

Einzelheiten zu den Berechtigungen

Der Dienst verwendet diese Richtlinie, um Aktionen für die folgenden Ressourcen durchzuführen:

- Schreibgeschützter IAM-Prinzipalzugriff: Gewährt einem Dienstbenutzer die Möglichkeit, schreibgeschützte Aktionen für vorhandene Ressourcen durchzuführen. AWS Security Incident Response
- IAM-Prinzipal-Schreibzugriff: Gewährt einem Dienstbenutzer die Möglichkeit, Ressourcen zu aktualisieren, zu ändern, zu löschen und zu erstellen. AWS Security Incident Response

Sie können die mit dieser Richtlinie verknüpften Berechtigungen unter AWS Verwaltete Richtlinien für AWSSecurityIncidentResponseFullAccesseinsehen.

AWS verwaltete Richtlinie: AWSSecurity IncidentResponseReadOnlyAccess

AWS Security Incident Response verwendet die AWSSecurity IncidentResponseReadOnlyAccess AWS verwaltete Richtlinie. Die Richtlinie gewährt nur Lesezugriff auf Ressourcen für Servicefälle. Sie können diese Richtlinie zusammen mit Ihren IAM-Prinzipalen verwenden, um schnell Berechtigungen für hinzuzufügen. AWS Security Incident Response

> **Important**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen in Tags. AWS Security Incident Response verwendet Tags, um Ihnen Verwaltungsdienste zur Verfügung zu stellen. Tags sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden

Einzelheiten zu den Berechtigungen

Der Dienst verwendet diese Richtlinie, um Aktionen für die folgenden Ressourcen durchzuführen:

- Schreibgeschützter IAM-Prinzipalzugriff: Gewährt einem Dienstbenutzer die Möglichkeit, schreibgeschützte Aktionen für vorhandene Ressourcen durchzuführen. AWS Security Incident Response

Sie können die mit dieser Richtlinie verknüpften Berechtigungen unter Verwaltete Richtlinien für einsehen. AWS AWSSecurityIncidentResponseReadOnlyAccess

AWS verwaltete Richtlinie: AWSSecurity IncidentResponseCaseFullAccess

AWS Security Incident Response verwendet die AWSSecurity IncidentResponseCaseFullAccess AWS verwaltete Richtlinie. Die Richtlinie gewährt vollen Zugriff auf Ressourcen für Servicefälle. Sie können diese Richtlinie zusammen mit Ihren IAM-Prinzipalen verwenden, um schnell Berechtigungen für hinzuzufügen. AWS Security Incident Response

> **Important**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen in Tags. AWS Security Incident Response verwendet Tags, um Ihnen Verwaltungsdienste zur Verfügung zu stellen. Tags sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden

Einzelheiten zu den Berechtigungen

Der Dienst verwendet diese Richtlinie, um Aktionen für die folgenden Ressourcen durchzuführen:

- Schreibgeschützter IAM-Prinzipalzugriff: Gewährt einem Servicebenutzer die Möglichkeit, schreibgeschützte Aktionen für bestehende Fälle durchzuführen. AWS Security Incident Response
- Schreibzugriff im IAM-Prinzipalfall: Gewährt einem Servicebenutzer die Möglichkeit, Fälle zu aktualisieren, zu ändern, zu löschen und zu erstellen. AWS Security Incident Response

Sie können die mit dieser Richtlinie verknüpften Berechtigungen unter AWS Verwaltete Richtlinien für AWSSecurityIncidentResponseCaseFullAccesseinsehen.

AWS verwaltete Richtlinie: AWSSecurity IncidentResponseTriageServiceRolePolicy

AWS Security Incident Response verwendet die AWSSecurity IncidentResponseTriageServiceRolePolicy AWS verwaltete Richtlinie. Diese AWS verwaltete Richtlinie ist der AWSServiceRoleForSecurityIncidentResponse_Triagedienstbezogenen Rolle zugeordnet.

Die Richtlinie bietet Zugriff darauf, Ihre Umgebung kontinuierlich auf Sicherheitsbedrohungen AWS Security Incident Response zu überwachen, Sicherheitsdienste zu optimieren, um Warngeräusche zu reduzieren, und Informationen zur Untersuchung potenzieller Vorfälle zu sammeln. Sie können diese Richtlinie nicht mit Ihren IAM-Entitäten verknüpfen.

> **Important**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche oder sensible Informationen in Tags. AWS Security Incident Response verwendet Tags, um Ihnen Verwaltungsdienste zur Verfügung zu stellen. Tags sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden

Einzelheiten zu den Berechtigungen

Der Dienst verwendet diese Richtlinie, um Aktionen für die folgenden Ressourcen durchzuführen:

- Ereignisse: Ermöglicht dem Service, eine von Amazon EventBridge verwaltete Regel zu erstellen. Diese Regel ist die Infrastruktur, die in Ihrem AWS Konto erforderlich ist, um Ereignisse von Ihrem Konto an den Service zu übertragen. Diese Aktion wird für jede AWS Ressource ausgeführt, die von verwaltet wird`triage.security-ir.amazonaws.com`.
- Amazon GuardDuty: Ermöglicht dem Service, Sicherheitsdienste zu optimieren, um Warngeräusche zu reduzieren, Informationen zur Untersuchung potenzieller Vorfälle zu sammeln und GuardDuty Malware-Scans einzuleiten.
- AWS Security Hub CSPM: Ermöglicht dem Service, aktivierte Standards und Produktintegrationen aufzulisten, Organisationsmitglieder und Administratorkonten aufzulisten und Sicherheitsdienste zu optimieren, um Warnmeldungen zu reduzieren und Informationen zur Untersuchung potenzieller Vorfälle zu sammeln.
- AWS Identity and Access Management: Ermöglicht dem Dienst, Rolleninformationen für die mit dem Dienst `AWSServiceRoleForAmazonGuardDutyMalwareProtection` verknüpfte Rolle abzurufen, um zu überprüfen, ob sie konfiguriert GuardDuty MalwareProtection ist.
- AWS Security Incident Response: Ermöglicht dem Service, Fälle zu erstellen und zu aktualisieren und Ressourcen zu taggen, beschränkt auf Ressourcen, die mit `SecurityIncidentResponseManaged=true` gekennzeichnet sind. Ermöglicht dem Dienst das Lesen von Mitgliedschaftsinformationen (GetMembership, ListMemberships).

Sie können die mit dieser Richtlinie verknüpften Berechtigungen unter AWS Verwaltete Richtlinien für einsehen [AWSSecurityIncidentResponseTriageServiceRolePolicy](#).

AWS Security Incident Response Aktualisierungen SLRs und verwaltete Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS Security Incident Response SLRs und verwalteten Richtlinienrollen seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst.

Änderungen	Beschreibung	Date
Aktualisiert — AWSSecurityIncidentResponseTriageServiceRolePolicy	Die Richtlinie ermöglicht es dem Dienst nun, GuardDuty Filter, die mit gekennzeichnet sind`SecurityIncidentResponseManaged=true` , zu ändern, die Detektorkonfigurationen zu aktualisieren und GuardDuty Malware-Scans zu starten. Es ermöglicht dem Dienst, Regeln zu erstellen und zu verwalten, die automatisch auf die Ergebnisse des Security Hub CSPM reagieren, und die Organisationsstruktur zu verstehen.	27. März 2026
Aktualisiert — AWSSecurityIncidentResponseServiceRolePolicy	Die Richtlinie führt jetzt Aktionen für die folgenden Ressourcen durch: ListCases: Ermöglicht dem KI-Agenten des Dienstes, Fälle für Sicherheitsuntersuchungen einzusehen UpdateCase: Ermöglicht dem KI-Agenten des Dienstes, die Fallmetadaten zu aktualisieren. CreateCaseComment: Ermöglicht dem KI-Agenten des Dienstes, seine Ergebnisse als Fallkommentar zu veröffentlichen ListComments: Ermöglicht dem KI-Agenten des Dienstes, Fallkommentare einzusehen, die für die Durchführung automatisierter Untersuchungen erforderlich sind	November 2025
Aktualisiert — AWSSecurityIncidentResponse	Die Richtlinie umfasst nun zwei neue Aktionen `"organizations:ListDelegatedAdministrators"` und eine neue Bedingung: `"organizations:DescribeAccount"`	November 2025

Änderungen	Beschreibung	Date

ServiceRolePolicy	<pre>"Condition": {
	      "StringEquals": {
	        "aws:ResourceAccount": "${aws:PrincipalAccount}"
	      }
	    }</pre>	

Aktualisierungen für SLR, mit denen Berechtigungen zur Unterstützung von Servicebe rechtigungen hinzugefügt werden.	AWSSecurityIncidentResponseTriageServiceRolePolicywurde aktualisiert und fügt nun die Berechtigungen security-ir:GetMembership, security-ir:, security-ir:ListMemberships, guardduty:, guarduty:UpdateCase, guardduty : und guardduty: ListFilters hinzugefügt. guardduty: wurde hinzugefügtUpdateFilter, um die Verwaltung von DeleteFilter Autoarchivierungsfiltern in delegierten Konten zu erleichtern. GetAdministratorAccount GetAdministratorAccount GuardDuty	02. Juni 2025
Neue Spiegelre flexkamera — AWSServiceRoleForSecurityIncidentResponse Neue verwaltete Richtlinie — AWSSecurityIncidentResponseServiceRolePolicy.	Neue dienstbezogene Rolle und angehängte Richtlinie, die den Dienstzugriff auf Ihre AWS Organizations Konten ermöglichen, um die Mitgliedschaft zu identifizieren.	01. Dezember 2024

Änderungen	Beschreibung	Date
Neue Spiegelre flexkamera — AWSServic eRoleForS ecurityIn cidentRes ponse_Triage Neue verwaltet e Richtlinie — AWSSecuri tyInciden tResponse TriageSer viceRolePolicy	Neue dienstbezogene Rolle und beigefügte Richtlinie, die den Dienstzugriff auf Ihre AWS Organizations Konten ermöglicht, um Sicherheitsereignisse zu sortieren.	01. Dezember 2024
Neue verwaltet e Richtlinie — AWSSecuri tyInciden tResponse FullAccess	AWS Security Incident Response eine neue Spiegelre flexkamera hinzufügen, die an IAM-Prinzipale für Lese- und Schreibaktionen für den Dienst angehängt wird.	01. Dezember 2024
Neue Rolle für verwaltet e Richtlinien — AWSSecuri tyInciden tResponse ReadOnlyAccess	AWS Security Incident Response eine neue Spiegelre flexkamera hinzufügen, die für Leseaktionen an IAM-Prinz ipale angehängt wird	01. Dezember 2024

Änderungen	Beschreibung	Date
Neue Rolle für verwaltete Richtlinien — AWSSecurityIncidentResponseCaseFullAccess	AWS Security Incident Response fügt eine neue Spiegelreflexkamera hinzu, die an IAM-Prinzipale angehängt wird, um Lese- und Schreibaktionen für Servicefälle durchzuführen.	01. Dezember 2024
Die Nachverfolgung von Änderungen wurde gestartet.	Mit der Nachverfolgung von Änderungen für AWS Security Incident Response SLRs und der Verwaltung von Richtlinien wurde begonnen	01. Dezember 2024

Vorfallreaktion

Sicherheit und Compliance liegen in der gemeinsamen AWS Verantwortung des Kunden. Dieses gemeinsame Modell kann dazu beitragen, den Kunden beim AWS Betrieb, der Verwaltung und der Kontrolle der Komponenten vom Host-Betriebssystem über die Virtualisierungsebene bis hin zur physischen Sicherheit der Einrichtungen, in denen der Service betrieben wird, zu entlasten. Der Kunde übernimmt die Verantwortung und Verwaltung des Gastbetriebssystems (einschließlich Updates und Sicherheitspatches), anderer zugehöriger Anwendungssoftware sowie der Konfiguration der AWS bereitgestellten Sicherheitsgruppen-Firewall. Weitere Informationen finden Sie im Modell der AWS gemeinsamen Verantwortung.

Indem Sie eine Sicherheitsgrundlage schaffen, die den Anforderungen Ihrer in der Cloud betriebenen Anwendungen entspricht, können Sie Abweichungen erkennen und entsprechend darauf reagieren. Da die Reaktion auf Sicherheitsvorfälle ein komplexes Thema sein kann, empfehlen wir Ihnen, die folgenden Ressourcen zu lesen, damit Sie besser verstehen, welche Auswirkungen die Reaktion auf Vorfälle und Ihre Entscheidungen auf Ihre Unternehmensziele haben: Whitepaper zu Best Practices zur AWS Sicherheit und Whitepaper Security Perspective of the AWS Cloud Adoption Framework (CAF).

Compliance-Validierung

Externe Prüfer bewerten die Sicherheit und Konformität von AWS Services im Rahmen mehrerer AWS Compliance-Programme. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Eine Liste der AWS Dienstleistungen im Rahmen bestimmter Compliance-Programme finden Sie unter AWS Dienstleistungen im Umfang der einzelnen Compliance-Programme. Allgemeine Informationen finden Sie unter AWS Compliance-Programme.

Mit AWS Artifact können Sie Prüfberichte von Drittanbietern herunterladen. Weitere Informationen finden Sie unter Berichte in AWS Artifact herunterladen.

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung von AWS Diensten 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 Umgebungen beschrieben, auf denen auf Sicherheit und Compliance ausgerichtete Basisumgebungen eingerichtet werden. AWS
- Whitepaper „Architecting for HIPAA“ zu Sicherheit und Compliance — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-konforme Anwendungen entwickeln können. AWS
- AWS Compliance-Ressourcen — Eine Sammlung von Arbeitsmappen und Leitfäden, die je nach Branche und Standort gelten. and/or
- Evaluierung von Ressourcen mit AWS Config Rules im AWS Config Developer Guide — AWS Config; bewertet, wie gut Ihre Ressourcenkonfigurationen internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub — Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb AWS. Security Hub verwendet Sicherheitskontrollen, um Ihre AWS Ressourcen zu bewerten und Ihre Einhaltung der Sicherheitsstandards und Best Practices der Sicherheitsbranche zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.
- Amazon GuardDuty — Dieser AWS Service erkennt potenzielle Bedrohungen für Ihre AWS Konten, Workloads, Container und Daten, indem er Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem wir die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllen.

- AWS Audit Manager — Mit diesem AWS Service können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um Ihr Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Protokollierung und Überwachung in AWS Security Incident Response

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer AWS Security Incident Response anderen AWS Lösungen. AWS Security Incident Response unterstützt derzeit die folgenden AWS Dienste zur Überwachung Ihres Unternehmens und der darin stattfindenden Aktivitäten.

AWS CloudTrail — Mit können CloudTrail Sie API-Aufrufe von der AWS Security Incident Response-Konsole aus erfassen. Wenn sich ein Benutzer beispielsweise authentifiziert, CloudTrail kann er Details wie die IP-Adresse in der Anfrage, wer die Anfrage gestellt hat und wann sie gestellt wurde, aufzeichnen.

Amazon CloudWatch Metrics — Mit CloudWatch Metriken können Sie Ereignisse nahezu in Echtzeit überwachen, melden und automatische Maßnahmen ergreifen. Sie können beispielsweise CloudWatch Dashboards zu den bereitgestellten Metriken erstellen, um Ihre AWS Security Incident Response Nutzung zu überwachen, oder Sie können CloudWatch Alarme für die bereitgestellten Metriken einrichten, um Sie bei Überschreitung eines festgelegten Schwellenwerts zu benachrichtigen.

Der Namespace für den Service ist AWS/Usage/. ServiceName Die verfügbaren Metriknamen sind und. ActiveManagedCases SelfManagedCases

Gemäß den AWS Servicebedingungen hat das AWS Security Incident Response Responder-Team Zugriff auf Ihre Historie von VPC- CloudTrail, DNS- und S3-Protokolldaten. Diese Daten können bei aktiven Sicherheitsvorfällen verwendet werden, wenn ein Fall im Security Incident AWS Response-Serviceportal noch offen ist.

Ausfallsicherheit

Die AWS globale Infrastruktur basiert auf 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 zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Sicherheit der Infrastruktur

AWS Security Incident Response ist durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff AWS Security Incident Response über das Netzwerk. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Oder Sie können den AWS Security Token Service (AWS STS) verwenden, um temporäre Sicherheitsanmeldeinformationen zum Signieren von Anfragen zu generieren.

Konfigurations- und Schwachstellenanalyse

Sie sind für die Verwaltung der Service-Containment-Rollen und der zugehörigen CloudFormation Stack-Sets verantwortlich.

AWS kümmert sich um grundlegende Sicherheitsaufgaben wie das Patchen von Gastbetriebssystemen (OS) und Datenbanken, die Firewall-Konfiguration und die Notfallwiederherstellung. Diese Verfahren wurden von qualifizierten Dritten überprüft und zertifiziert. Weitere Informationen finden Sie in den folgenden AWS -Ressourcen:

- Modell der geteilten Verantwortung
- Bewährte Methoden für Sicherheit, Identität und Compliance

Serviceübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine juristische Stelle, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine privilegiertere juristische Stelle zwingen kann, die Aktion auszuführen. Im Fall AWS eines dienstübergreifenden Identitätswechsels kann es zu einem Problem mit dem verwirrten Stellvertreter kommen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der Anruf-Dienst kann so manipuliert werden, dass er seine Berechtigungen verwendet, um auf die Ressourcen eines anderen Kunden zu reagieren, auf die er sonst nicht zugreifen dürfte. Um dies zu verhindern, AWS bietet Tools, mit denen Sie Ihre Daten für alle Dienste mit Dienstprinzipalen schützen können, denen Zugriff auf Ressourcen in Ihrem Konto gewährt wurde.

Wir empfehlen die Verwendung der SourceAccount globalen Bedingungskontextschlüssel AWSAWS: SourceArn und: in Ressourcenrichtlinien, um die Berechtigungen einzuschränken, die Amazon Connect einem anderen Service für die Ressource erteilt. Wenn Sie beide Kontextschlüssel für globale Bedingungen verwenden, müssen der SourceAccount Wert AWS: und das Konto im SourceArn Wert AWS: dieselbe Konto-ID verwenden, wenn sie in derselben Richtlinienerklärung verwendet werden.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des exakten Amazon-Ressourcennamens (ARN) der Ressource, die Sie zulassen möchten. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den AWS SourceArn globalen Kontextbedingungsschlüssel mit Platzhaltern (*) für die unbekannten Teile des ARN. Zum Beispiel arn ::servicename: :region-name AWS: :your account ID: *. AWS

Ein Beispiel für eine Richtlinie zur Übernahme einer Rolle, die zeigt, wie Sie verhindern können, dass ein Stellvertreter verwirrt ist, finden Sie unter Richtlinie zur Verhinderung verwirrter Stellvertreter.

Service Quotas

AWS Security Incident Response

Das AWS allgemeine Referenzhandbuch enthält die aktuellsten AWS Security Incident Response Endpunkte und Kontingente.

AWS Security Incident Response Technischer Leitfaden

Inhalt

Überblick

Dieser Leitfaden bietet einen Überblick über die Grundlagen der Reaktion auf Sicherheitsvorfälle in der Amazon Web Services (AWS) Cloud-Umgebung eines Kunden. Er bietet einen Überblick über Konzepte zur Cloudsicherheit und zur Reaktion auf Vorfälle und identifiziert Cloudfunktionen, -services und -mechanismen, die Kunden zur Verfügung stehen, die auf Sicherheitsprobleme reagieren.

Dieser Leitfaden richtet sich an Personen in technischen Funktionen und setzt voraus, dass Sie mit den allgemeinen Prinzipien der Informationssicherheit vertraut sind, über grundlegende Kenntnisse der Reaktion auf Sicherheitsvorfälle in Ihren aktuellen lokalen Umgebungen verfügen und mit Cloud-Diensten vertraut sind.

Sind Sie Well-Architected?

Das AWS Well-Architected Framework hilft Ihnen dabei, die Vor- und Nachteile der Entscheidungen zu verstehen, die Sie beim Aufbau von Systemen in der Cloud treffen. Die sechs Säulen des

Frameworks ermöglichen es Ihnen, bewährte Architekturpraktiken für den Entwurf und Betrieb zuverlässiger, sicherer, effizienter, kostengünstiger und nachhaltiger Systeme kennenzulernen. Mithilfe des AWS Well-Architected Tool, das kostenlos in der AWS Well-Architected Tool Konsole verfügbar ist, können Sie Ihre Workloads anhand dieser bewährten Methoden überprüfen, indem Sie für jede Säule eine Reihe von Fragen beantworten.

Weitere Expertentipps und bewährte Methoden für Ihre Cloud-Architektur — Referenzarchitekturbereitstellungen, Diagramme und Whitepapers — finden Sie im Architecture Center.AWS

Einführung

Sicherheit hat bei oberste Priorität AWS. AWS Kunden profitieren von Rechenzentren und einer Netzwerkarchitektur, die darauf ausgelegt sind, die Bedürfnisse der sicherheitssensibelsten Unternehmen zu erfüllen. AWS hat ein Modell der gemeinsamen Verantwortung: AWS verwaltet die Sicherheit der Cloud, und die Kunden sind für die Sicherheit in der Cloud verantwortlich. Das bedeutet, dass Sie die volle Kontrolle über Ihre Sicherheitsimplementierung haben, einschließlich des Zugriffs auf verschiedene Tools und Dienste, mit denen Sie Ihre Sicherheitsziele erreichen können. Diese Funktionen helfen Ihnen dabei, eine Sicherheitsgrundlage für Anwendungen zu schaffen, die in der ausgeführt AWS Cloud werden.

Wenn eine Abweichung von der Basislinie auftritt, z. B. durch eine Fehlkonfiguration oder sich ändernde externe Faktoren, müssen Sie reagieren und Nachforschungen anstellen. Um dies erfolgreich zu tun, müssen Sie die grundlegenden Konzepte der Reaktion auf Sicherheitsvorfälle in Ihrer AWS Umgebung und die Anforderungen zur Vorbereitung, Schulung und Schulung von Cloud-Teams verstehen, bevor Sicherheitsprobleme auftreten. Es ist wichtig zu wissen, welche Kontrollen und Funktionen Sie verwenden können, aktuelle Beispiele für die Lösung potenzieller Probleme zu finden und Lösungsmethoden zu identifizieren, die mithilfe von Automatisierung die Reaktionsgeschwindigkeit und Konsistenz verbessern. Darüber hinaus sollten Sie Ihre Compliance- und regulatorischen Anforderungen in Bezug auf den Aufbau eines Programms zur Reaktion auf Sicherheitsvorfälle zur Erfüllung dieser Anforderungen verstehen.

Die Reaktion auf Sicherheitsvorfälle kann komplex sein, daher empfehlen wir Ihnen, einen iterativen Ansatz zu verfolgen: Beginnen Sie mit den wichtigsten Sicherheitsdiensten, bauen Sie grundlegende Erkennungs- und Reaktionsfunktionen auf und entwickeln Sie dann Playbooks, um eine erste Bibliothek von Mechanismen zur Reaktion auf Vorfälle zu erstellen, die dann wiederholt und verbessert werden können.

Bevor Sie beginnen

Machen Sie sich mit den relevanten Standards und Frameworks für Sicherheit und Reaktion auf Sicherheitsvorfälle vertraut AWS, bevor Sie in beginnen, sich mit den entsprechenden Standards und Frameworks für die Reaktion auf AWS Sicherheitsvorfälle vertraut zu machen. Diese Grundlagen helfen Ihnen dabei, die in diesem Leitfaden vorgestellten Konzepte und bewährten Methoden zu verstehen.

AWS Sicherheitsstandards und Frameworks

Zu Beginn empfehlen wir Ihnen, die Whitepaper Best Practices for Security, Identity and Compliance, Security Pillar — AWS Well-Architected Framework und The Security Perspective of the Overview of the AWS Cloud Adoption Framework (AWS CAF) zu lesen.

Das AWS CAF bietet Leitlinien zur Unterstützung der Koordination zwischen verschiedenen Teilen von Unternehmen, die auf die Cloud umsteigen. Die AWS CAF-Leitlinien sind in mehrere Schwerpunktbereiche unterteilt, die als Perspektiven bezeichnet werden und für den Aufbau cloudbasierter IT-Systeme relevant sind. Die Sicherheitsperspektive beschreibt, wie ein Sicherheitsprogramm für mehrere Arbeitsbereiche implementiert werden kann. Einer davon ist die Reaktion auf Vorfälle. Dieses Dokument ist das Ergebnis unserer Erfahrungen in der Zusammenarbeit mit Kunden, um sie bei der Entwicklung effektiver und effizienter Programme und Funktionen zur Reaktion auf Sicherheitsvorfälle zu unterstützen.

Branchenübliche Standards und Rahmenbedingungen für die Reaktion auf Vorfälle

Dieses Whitepaper folgt den Standards und bewährten Verfahren zur Reaktion auf Vorfälle aus dem Computer Security Incident Handling Guide SP 800-61 r3, der vom National Institute of Standards and Technology (NIST) erstellt wurde. Das Lesen und Verstehen der von NIST eingeführten Konzepte ist eine hilfreiche Voraussetzung. Konzepte und bewährte Verfahren aus diesem NIST-Leitfaden werden in diesem paper auf AWS Technologien angewendet. Vorfallszenarien vor Ort fallen jedoch nicht in den Anwendungsbereich dieses Leitfadens.

AWS Überblick über die Reaktion auf Vorfälle

Zunächst ist es wichtig zu verstehen, wie sich Sicherheitsabläufe und Reaktion auf Vorfälle in der Cloud unterscheiden. Um effektive Reaktionsmöglichkeiten zu entwickeln AWS, müssen Sie die Abweichungen von der herkömmlichen Reaktion vor Ort und deren Auswirkungen auf Ihr Incident-Response-Programm verstehen. Jeder dieser Unterschiede sowie die wichtigsten Prinzipien der Planung von AWS Incident-Response-Konzepten werden in diesem Abschnitt detailliert beschrieben.

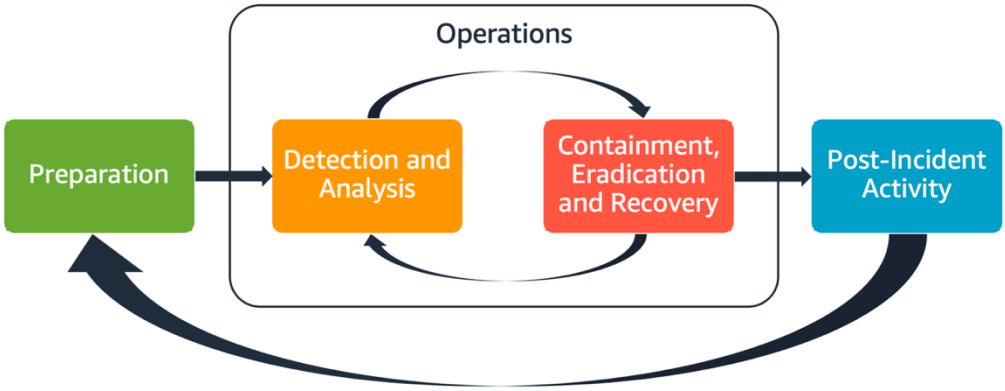
Aspekte der Reaktion auf AWS Vorfälle

Alle AWS Benutzer innerhalb eines Unternehmens sollten ein grundlegendes Verständnis der Prozesse zur Reaktion auf Sicherheitsvorfälle haben, und das Sicherheitspersonal sollte wissen, wie auf Sicherheitsprobleme reagiert werden muss. Ausbildung, Schulung und Erfahrung sind für ein erfolgreiches Programm zur Reaktion auf Cloud-Vorfälle von entscheidender Bedeutung und werden idealerweise schon lange vor einem möglichen Sicherheitsvorfall implementiert. Die Grundlage für ein erfolgreiches Incident-Response-Programm in der Cloud bilden die Vorbereitung, der Betrieb und die Aktivitäten nach dem Vorfall.

Im Folgenden werden diese Aspekte genauer beschrieben:

- Vorbereitung — Bereiten Sie Ihr Incident-Response-Team darauf vor, interne Vorfälle zu erkennen und darauf zu reagieren, AWS indem Sie detektivische Kontrollen aktivieren und den angemessenen Zugriff auf die erforderlichen Tools und Cloud-Dienste überprüfen. Bereiten Sie außerdem die erforderlichen Playbooks vor, sowohl manuell als auch automatisiert, um zuverlässige und konsistente Reaktionen auf Vorfälle zu gewährleisten.
- Operativer Betrieb — Reaktion auf Sicherheitsereignisse und potenzielle Vorfälle gemäß den Phasen der Reaktion auf Vorfälle durch NIST: Erkennung, Analyse, Eindämmung, Beseitigung und Wiederherstellung.
- Aktivitäten nach einem Vorfall — Verbessern Sie die Ergebnisse Ihrer Sicherheitsereignisse und Simulationen, um die Effizienz Ihrer Reaktion zu verbessern, den Nutzen aus Reaktion und Untersuchung zu erhöhen und das Risiko weiter zu reduzieren. Sie müssen aus Vorfällen lernen und die Verantwortung für Verbesserungsmaßnahmen für klar definiert sein.

Jeder dieser Aspekte wird in diesem Leitfaden untersucht und detailliert beschrieben. Das folgende Diagramm zeigt den Ablauf dieser Aspekte, wobei es sich an dem bereits erwähnten NIST-Lebenszyklus für die Reaktion auf Vorfälle orientiert, jedoch mit Vorgängen, die die Erkennung und Analyse sowie die Eindämmung, Beseitigung und Wiederherstellung umfassen.



Aspekte der Reaktion auf AWS Vorfälle

AWS Prinzipien und Entwurfsziele für die Reaktion auf Vorfälle

Die allgemeinen Verfahren und Mechanismen der Reaktion auf Sicherheitsvorfälle, wie sie im NIST SP 800-61 Leitfaden zur Behandlung von Sicherheitsvorfällen definiert sind, sind zwar solide, wir empfehlen Ihnen jedoch, auch die folgenden spezifischen Entwurfsziele zu berücksichtigen, die für die Reaktion auf Sicherheitsvorfälle in einer Cloud-Umgebung relevant sind:

- Festlegung von Reaktionszielen — Arbeiten Sie mit Interessenvertretern, Rechtsberatern und der Unternehmensleitung zusammen, um das Ziel festzulegen, mit dem auf einen Vorfall reagiert werden soll. Zu den gemeinsamen Zielen gehören die Eindämmung und Minderung des Problems, die Wiederherstellung der betroffenen Ressourcen, die Aufbewahrung von Daten für die Forensik, die Rückkehr zu bekanntermaßen sicheren Abläufen und letztlich das Lernen aus Vorfällen.
- Reagieren Sie mithilfe der Cloud — Implementieren Sie Reaktionsmuster innerhalb der Cloud, wo das Ereignis und die Daten auftreten.
- Wissen Sie, was Sie haben und was Sie benötigen — Bewahren Sie Protokolle, Ressourcen, Schnappschüsse und andere Beweise auf, indem Sie sie kopieren und in einem zentralen Cloud-Konto speichern, das speziell für die Reaktion vorgesehen ist. Verwenden Sie Tags, Metadaten und Mechanismen, die Aufbewahrungsrichtlinien erzwingen. Sie müssen verstehen, welche Dienste Sie verwenden, und dann die Anforderungen für die Untersuchung dieser Dienste ermitteln. Um Ihre Umgebung besser zu verstehen, können Sie auch Tagging verwenden, auf das weiter unten in diesem Dokument in diesem the section called “Entwickeln und Implementieren einer Markierungsstrategie” Abschnitt eingegangen wird.
- Verwenden Sie Mechanismen zur erneuten Bereitstellung — Wenn eine Sicherheitsanomalie auf eine Fehlkonfiguration zurückzuführen ist, kann die Behebung so einfach sein wie das Entfernen der Varianz durch erneutes Bereitstellen von Ressourcen mit der richtigen Konfiguration. Wenn

eine mögliche Gefährdung festgestellt wird, stellen Sie sicher, dass Ihre erneute Bereitstellung eine erfolgreiche und verifizierte Abmilderung der Hauptursachen beinhaltet.

- Automatisieren Sie, wo immer möglich: Wenn Probleme auftreten oder sich wiederholen, sollten Sie Mechanismen entwickeln, um häufig auftretende Ereignisse programmatisch zu analysieren und darauf zu reagieren. Verwenden Sie menschliche Antworten für einzigartige, komplexe oder sensible Vorfälle, bei denen die Automatisierung nicht ausreicht.
- Entscheiden Sie sich für skalierbare Lösungen — Bemühen Sie sich, der Skalierbarkeit des Cloud-Computing-Ansatzes Ihres Unternehmens gerecht zu werden. Implementieren Sie Erkennungs- und Reaktionsmechanismen, die sich auf Ihre Umgebungen skalieren lassen, um die Zeit zwischen Erkennung und Reaktion effektiv zu verkürzen.
- Lernen Sie Ihren Prozess kennen und verbessern Sie ihn — Identifizieren Sie proaktiv Lücken in Ihren Prozessen, Tools oder Mitarbeitern und implementieren Sie einen Plan, um diese zu beheben. Simulationen sind sichere Methoden, um Lücken zu finden und Prozesse zu verbessern. Einzelheiten zur Iteration Ihrer Prozesse finden Sie im the section called “Aktivität nach Vorfällen” Abschnitt dieses Dokuments.

Diese Entwurfsziele sollen als Erinnerung daran dienen, Ihre Architekturimplementierung daraufhin zu überprüfen, ob sie sowohl zur Reaktion auf Vorfälle als auch zur Bedrohungserkennung in der Lage ist. Denken Sie bei der Planung Ihrer Cloud-Implementierungen darüber nach, auf einen Vorfall zu reagieren, idealerweise mit einer forensisch fundierten Reaktionsmethode. In einigen Fällen bedeutet dies, dass Sie möglicherweise mehrere Organisationen, Konten und Tools haben, die speziell für diese Reaktionsaufgaben eingerichtet wurden. Diese Tools und Funktionen sollten der für Vorfälle verantwortlichen Person über die Bereitstellungspipeline zur Verfügung gestellt werden. Sie sollten nicht statisch sein, da dies zu einem größeren Risiko führen kann.

Domänen für Sicherheitsvorfälle in der Cloud

Um sich effektiv auf Sicherheitsereignisse in Ihrer AWS Umgebung vorbereiten und darauf reagieren zu können, müssen Sie die häufigsten Arten von Cloud-Sicherheitsvorfällen kennen. In der Verantwortung des Kunden gibt es drei Bereiche, in denen Sicherheitsvorfälle auftreten können: Service, Infrastruktur und Anwendung. Verschiedene Bereiche erfordern unterschiedliche Kenntnisse, Tools und Reaktionsprozesse. Betrachten Sie diese Domänen:

- Dienstdomäne — Vorfälle in der Dienstdomäne können sich auf Ihre AWS-KontoAWS Identity and Access Management(IAM-) Berechtigungen, Ressourcenmetadaten, die Abrechnung oder andere Bereiche auswirken. Ein Dienstdomänenereignis ist ein Ereignis, auf das Sie ausschließlich mit AWS API-Mechanismen reagieren oder bei dem Sie Hauptursachen im Zusammenhang mit

Ihrer Konfiguration oder Ihren Ressourcenberechtigungen haben und möglicherweise eine damit verbundene serviceorientierte Protokollierung haben.

- Infrastrukturdomäne — Zu Vorfällen in der Infrastrukturdomäne gehören daten- oder netzwerkbezogene Aktivitäten, wie Prozesse und Daten auf Ihren Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Datenverkehr zu Ihren Amazon EC2 EC2-Instances innerhalb der Virtual Private Cloud (VPC) und andere Bereiche, wie Container oder andere future Dienste. Ihre Reaktion auf Ereignisse in der Infrastrukturdomäne beinhaltet häufig die Erfassung von vorfallbezogenen Daten für forensische Analysen. Dies beinhaltet wahrscheinlich die Interaktion mit dem Betriebssystem einer Instanz und kann in verschiedenen Fällen auch API-Mechanismen beinhalten. AWS Im Infrastrukturbereich können Sie eine Kombination aus AWS APIs und DFIR-Tools (Digital forensics/incident Response) innerhalb eines Gastbetriebssystems verwenden, z. B. eine Amazon EC2 EC2-Instance, die für die Durchführung forensischer Analysen und Untersuchungen vorgesehen ist. Bei Infrastrukturdomänenvorfällen können Netzwerkpaketerfassungen, Festplattenblöcke auf einem Amazon Elastic Block Store (Amazon EBS) -Volume oder flüchtiger Speicher, der von einer Instance abgerufen wurde, analysiert werden.
- Anwendungsdomäne — Vorfälle in der Anwendungsdomäne treten im Anwendungscode oder in der Software auf, die für die Dienste oder die Infrastruktur bereitgestellt wird. Diese Domain sollte in Ihren Playbooks zur Erkennung und Abwehr von Cloud-Bedrohungen enthalten sein und könnte ähnliche Reaktionen wie die Infrastrukturdomäne beinhalten. Mit einer geeigneten und durchdachten Anwendungsarchitektur können Sie diese Domäne mithilfe von Cloud-Tools verwalten, indem Sie automatische Erfassung, Wiederherstellung und Bereitstellung nutzen.

Denken Sie in diesen Bereichen an die Akteure, die möglicherweise gegen AWS Konten, Ressourcen oder Daten vorgehen. Unabhängig davon, ob es sich um interne oder externe Risiken handelt, verwenden Sie einen Risikorahmen, um spezifische Risiken für das Unternehmen zu ermitteln und sich entsprechend vorzubereiten. Darüber hinaus sollten Sie Bedrohungsmodelle entwickeln, die Ihnen bei der Planung Ihrer Reaktion auf Vorfälle und beim Aufbau einer durchdachten Architektur helfen können.

Die wichtigsten Unterschiede bei der Reaktion auf Vorfälle sind AWS

Die Reaktion auf Vorfälle ist ein integraler Bestandteil einer Cybersicherheitsstrategie, entweder vor Ort oder in der Cloud. Sicherheitsprinzipien wie geringste Rechte und umfassende Abwehr zielen darauf ab, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten sowohl vor Ort als auch in der Cloud zu schützen. Es folgen mehrere Muster zur Reaktion auf Vorfälle, die diese Sicherheitsprinzipien unterstützen, darunter die Aufbewahrung von Protokollen, die Auswahl

von Warnmeldungen anhand von Bedrohungsmodellen, die Entwicklung von Playbooks und die Integration von Sicherheitsinformationen und Ereignismanagement (SIEM). Die Unterschiede beginnen, wenn Kunden beginnen, diese Muster in der Cloud zu entwerfen und zu entwickeln. Im Folgenden sind die wichtigsten Unterschiede bei der Reaktion auf Vorfälle in AWS aufgeführt.

Unterschied #1: Sicherheit als gemeinsame Verantwortung

Die Verantwortung für Sicherheit und Einhaltung der Vorschriften wird von AWS den Kunden gemeinsam getragen. Dieses Modell der geteilten Verantwortung entlastet den Kunden teilweise, da AWS die Komponenten vom Host-Betriebssystem und der Virtualisierungsebene bis hin zur physischen Sicherheit der Einrichtungen, in denen der Service betrieben wird, verwaltet und kontrolliert werden. Weitere Informationen zum Modell der gemeinsamen Verantwortung finden Sie in der Dokumentation zum Modell der gemeinsamen Verantwortung.

Wenn sich Ihre gemeinsame Verantwortung in der Cloud ändert, ändern sich auch Ihre Optionen für die Reaktion auf Vorfälle. Diese Kompromisse zu planen und zu verstehen und sie mit Ihren Governance-Anforderungen in Einklang zu bringen, ist ein entscheidender Schritt bei der Reaktion auf Vorfälle.

Zusätzlich zu der direkten Beziehung, zu der Sie stehen AWS, gibt es möglicherweise andere Entitäten, die in Ihrem jeweiligen Verantwortungsmodell Verantwortung übernehmen. Beispielsweise könnten Sie interne Organisationseinheiten haben, die Verantwortung für einige Aspekte Ihrer Geschäftstätigkeit übernehmen. Möglicherweise haben Sie auch Beziehungen zu anderen Parteien, die einen Teil Ihrer Cloud-Technologie entwickeln, verwalten oder betreiben.

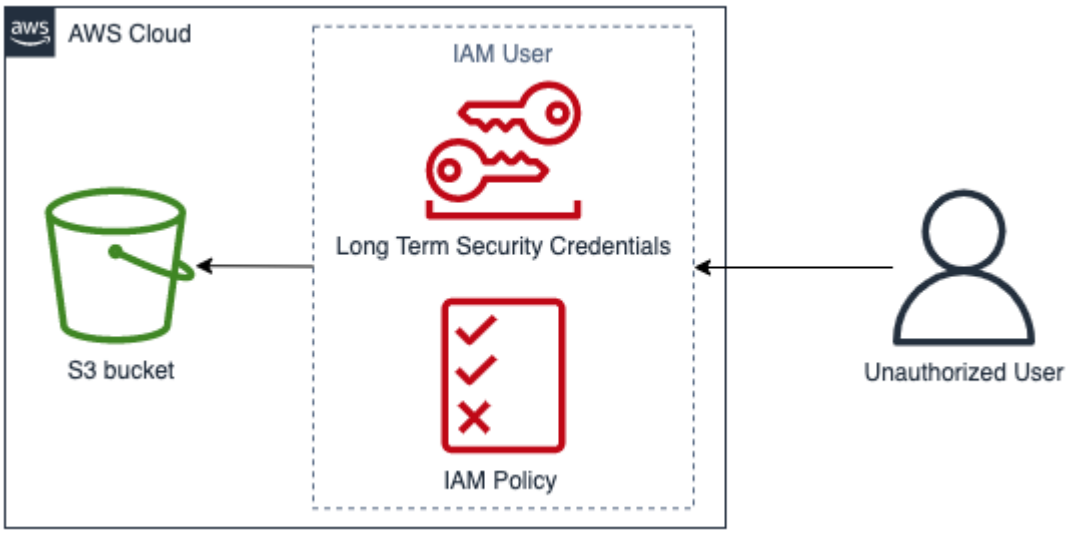
Es ist äußerst wichtig, einen geeigneten Plan zur Reaktion auf Vorfälle und entsprechende Playbooks zu erstellen und zu testen, die zu Ihrem Betriebsmodell passen.

Unterschied #2: Cloud-Dienstdomäne

Aufgrund der unterschiedlichen Sicherheitsverantwortung bei Cloud-Diensten wurde eine neue Domäne für Sicherheitsvorfälle eingeführt: die Dienstdomäne, die weiter oben im Abschnitt Incident-Domain erläutert wurde. Die Dienstdomäne umfasst das AWS Konto eines Kunden, IAM-Berechtigungen, Ressourcenmetadaten, Abrechnung und andere Bereiche. Diese Domain unterscheidet sich bei der Reaktion auf Vorfälle aufgrund der Art und Weise, wie Sie reagieren. Die Reaktion innerhalb der Dienstdomäne erfolgt in der Regel durch Überprüfung und Ausgabe von API-Aufrufen und nicht durch herkömmliche host- und netzwerkbasierte Antworten. In der Dienstdomäne werden Sie nicht mit dem Betriebssystem einer betroffenen Ressource interagieren.

Das folgende Diagramm zeigt ein Beispiel für ein Sicherheitsereignis in der Dienstdomäne, das auf einem architektonischen Anti-Pattern basiert. In diesem Fall erhält ein nicht autorisierter Benutzer

die langfristigen Sicherheitsanmeldedaten eines IAM-Benutzers. Der IAM-Benutzer verfügt über eine IAM-Richtlinie, die es ihm ermöglicht, Objekte aus einem Amazon Simple Storage Service (Amazon S3) -Bucket abzurufen. Um auf dieses Sicherheitsereignis AWS APIs zu reagieren, würden Sie AWS Protokolle wie AWS CloudTrailAmazon S3 S3-Zugriffsprotokolle analysieren. Sie würden es auch verwenden AWS APIs , um den Vorfall einzudämmen und ihn zu beheben.



Beispiel für eine Dienstdomäne

Unterschied #3: APIs für die Bereitstellung der Infrastruktur

Ein weiterer Unterschied ergibt sich aus den Cloud-Eigenschaften von On-Demand-Self-Service. Die Haupteinrichtung, mit der Kunden interagieren, AWS Cloud indem sie eine RESTful API über öffentliche und private Endpunkte verwenden, die an vielen geografischen Standorten auf der ganzen Welt verfügbar sind. Kunden können APIs mit AWS Anmeldeinformationen darauf zugreifen. Im Gegensatz zur lokalen Zugriffskontrolle sind diese Anmeldeinformationen nicht unbedingt an ein Netzwerk oder eine Microsoft Active Directory-Domäne gebunden. Anmeldeinformationen werden stattdessen einem IAM-Prinzipal innerhalb eines AWS Kontos zugeordnet. Auf diese API-Endpunkte kann auch außerhalb Ihres Unternehmensnetzwerks zugegriffen werden. Daher ist es wichtig, sich darüber im Klaren zu sein, wenn Sie auf einen Vorfall reagieren, bei dem Anmeldeinformationen außerhalb Ihres erwarteten Netzwerks oder Ihrer Region verwendet werden.

Aufgrund des API-basierten Charakters von AWS ist AWS CloudTrail es eine wichtige Protokollquelle für die Reaktion auf Sicherheitsereignisse. Sie verfolgt die in Ihren AWS Konten getätigten Verwaltungs-API-Aufrufe und enthält Informationen zum Quellort der API-Aufrufe.

Unterschied #4: Dynamischer Charakter der Cloud

Die Cloud ist dynamisch. Sie ermöglicht Ihnen das schnelle Erstellen und Löschen von Ressourcen. Mit der automatischen Skalierung können Ressourcen je nach Zunahme des Datenverkehrs hoch- und heruntergefahren werden. Bei einer kurzlebigen Infrastruktur und schnellen Änderungen ist eine Ressource, die Sie untersuchen, möglicherweise nicht mehr vorhanden oder wurde möglicherweise geändert. Für die Analyse von Vorfällen ist es wichtig, die kurzlebige Natur von AWS Ressourcen zu verstehen und zu verstehen, wie Sie die Erstellung und Löschung von AWS Ressourcen nachverfolgen können. Sie können AWS Configes verwenden, um den Konfigurationsverlauf Ihrer AWS Ressourcen nachzuverfolgen.

Unterschied #5: Datenzugriff

Der Datenzugriff ist auch in der Cloud anders. Sie können sich nicht an einen Server anschließen, um die Daten zu sammeln, die Sie für eine Sicherheitsuntersuchung benötigen. Daten werden drahtgebunden und über API-Aufrufe gesammelt. Sie müssen lernen und verstehen, wie die Datenerfassung durchgeführt wird, um auf diesen Wandel vorbereitet zu sein. APIs Außerdem müssen Sie sicherstellen, dass die richtige Speicherung für eine effektive Erfassung und einen effektiven Zugriff gewährleistet ist.

Unterschied #6: Bedeutung der Automatisierung

Damit Kunden die Vorteile der Cloud-Einführung voll ausschöpfen können, muss ihre Betriebsstrategie die Automatisierung umfassen. Infrastructure as Code (IaC) ist ein Muster hocheffizienter automatisierter Umgebungen, in denen AWS Dienste mithilfe von Code bereitgestellt, konfiguriert, neu konfiguriert und zerstört werden, der durch native IaC-Dienste AWS CloudFormationoder Lösungen von Drittanbietern ermöglicht wird. Dadurch wird die Implementierung der Reaktion auf Vorfälle stark automatisiert, was wünschenswert ist, um menschliche Fehler zu vermeiden, insbesondere beim Umgang mit Beweisen. Automatisierung wird zwar vor Ort eingesetzt, ist aber in der Regel unverzichtbar und einfacher. AWS Cloud

Beseitigung dieser Unterschiede

Um diese Unterschiede zu beheben, befolgen Sie die im nächsten Abschnitt beschriebenen Schritte, um sicherzustellen, dass Ihr Programm zur Reaktion auf Vorfälle, das Mitarbeiter, Prozesse und Technologien umfasst, gut vorbereitet ist.

Vorbereitung

Die Vorbereitung auf einen Vorfall ist entscheidend für eine zeitnahe und effektive Reaktion im Ernstfall. Die Vorbereitung erfolgt in drei Bereichen:

- Mitarbeiter — Um Ihre Mitarbeiter auf einen Sicherheitsvorfall vorzubereiten, müssen Sie die für die Reaktion auf Sicherheitsvorfälle relevanten Akteure identifizieren und sie in den Bereichen Incident Response und Cloud-Technologien schulen.
- Prozess — Um Ihre Prozesse auf einen Sicherheitsvorfall vorzubereiten, müssen Sie Architekturen dokumentieren, gründliche Pläne zur Reaktion auf Vorfälle entwickeln und Playbooks für eine konsistente Reaktion auf Sicherheitsvorfälle erstellen.
- Technologie — Um Ihre Technologie auf einen Sicherheitsvorfall vorzubereiten, müssen Sie den Zugriff einrichten, die erforderlichen Protokolle zusammenfassen und überwachen, effektive Warnmechanismen implementieren und Reaktions- und Ermittlungskapazitäten entwickeln.

Jeder dieser Bereiche ist für eine effektive Reaktion auf Vorfälle gleichermaßen wichtig. Ohne alle drei ist kein Vorfallreaktionsprogramm vollständig oder wirksam. Die Vorbereitung von Mitarbeitern, Prozessen und Technologien muss eng ineinandergreifen, um auf einen Vorfall vorbereitet zu sein.

Personen

Um auf ein Sicherheitsereignis reagieren zu können, müssen Sie die Beteiligten identifizieren, die die Reaktion auf ein Sicherheitsereignis unterstützen würden. Darüber hinaus ist es für eine effektive Reaktion von entscheidender Bedeutung, dass sie in Bezug auf AWS Technologien und Ihre AWS Umgebung geschult werden.

Definieren von Rollen und Zuständigkeiten

Der Umgang mit Sicherheitsereignissen erfordert organisationsübergreifende Disziplin und Handlungsbereitschaft. Innerhalb Ihrer Organisationsstruktur sollte es viele Personen geben, die für einen Vorfall verantwortlich und rechenschaftspflichtig sind sowie konsultiert oder auf dem Laufenden gehalten werden. Beispiele wären etwa Vertreter der Personalabteilung (HR), des Führungsteams und der Rechtsabteilung. Berücksichtigen Sie diese Rollen und Verantwortlichkeiten sowie die Frage, ob Dritte eingebunden werden müssen. Beachten Sie, dass es in vielen Regionen lokale Gesetze gibt, die regeln, was getan werden sollte und was nicht. Auch wenn es bürokratisch erscheinen mag, ein Diagramm mit Verantwortung, Rechenschaft, Konsultierung und Information (RACI) für Ihre Sicherheitspläne zu erstellen, ermöglicht dies eine schnelle und direkte Kommunikation und zeigt klar und deutlich, wie die Führung in den verschiedenen Phasen der Veranstaltung abläuft.

Während eines Vorfalls ist die Angabe der betroffenen Anwendungen und Ressourcen owners/developers von entscheidender Bedeutung, da es sich um Fachexperten (SMEs) handelt, die Informationen und den Kontext bereitstellen können, um die Auswirkungen zu messen. Üben Sie und bauen Sie Beziehungen zu den Entwicklern und Anwendungsbesitzern auf, bevor Sie sich bei der Vorfallreaktion auf deren Fachwissen verlassen. Anwendungseigentümer oder SMEs, wie z. B. Ihre Cloud-Administratoren oder Techniker, müssen möglicherweise in Situationen handeln, in denen die Umgebung unbekannt oder komplex ist oder in denen die Responder keinen Zugriff haben.

Schließlich können vertrauenswürdige Mitarbeiter in die Untersuchung oder Reaktion einbezogen werden, da sie zusätzliches Fachwissen und wertvolle Analysen bieten können. Wenn Sie in Ihrem eigenen Team nicht über diese Fähigkeiten verfügen, sollten Sie eine externe Partei mit der Unterstützung beauftragen.

Schulen Sie Mitarbeiter für die Reaktion auf Vorfälle

Die Schulung Ihrer Mitarbeiter zur Reaktion auf Vorfälle in Bezug auf die Technologien, die ihr Unternehmen einsetzt, ist entscheidend, damit sie angemessen auf ein Sicherheitsereignis reagieren können. Wenn Ihre Mitarbeiter die zugrundeliegenden Technologien nicht verstehen, kann es zu längeren Reaktionszeiten kommen. Neben den herkömmlichen Konzepten zur Reaktion auf Vorfälle ist es auch wichtig, dass sie die AWS Dienste und ihre AWS Umgebung verstehen. Es gibt eine Reihe traditioneller Mechanismen zur Schulung Ihres Notfallpersonals, z. B. Online-Schulungen und Präsenzschulungen. Sie sollten auch die Durchführung von Spieltagen oder Simulationen als Trainingsmechanismus in Betracht ziehen. Einzelheiten zur Durchführung von Simulationen finden Sie im the section called “Führen Sie regelmäßige Simulationen durch” Abschnitt dieses Dokuments.

AWS Cloud Technologien verstehen

Um Abhängigkeiten zu reduzieren und die Reaktionszeit zu verkürzen, sollten Sie sicherstellen, dass Ihre Sicherheitsteams und Einsatzkräfte über Cloud-Dienste informiert sind und die Möglichkeit haben, praktische Erfahrungen mit der spezifischen Cloud-Umgebung zu sammeln, die Ihr Unternehmen verwendet. Damit Incident Responder effektiv arbeiten können, ist es wichtig, die AWS Grundlagen, IAM AWS Organizations, AWS Protokollierungs- und Überwachungsdienste sowie Sicherheitsdienste zu verstehen. AWS

AWS bietet Online-Sicherheitsworkshops (siehe AWS Sicherheitsworkshops) an, in denen Sie praktische Erfahrungen mit AWS Sicherheits- und Überwachungsdiensten sammeln können. AWS bietet außerdem eine Reihe von Schulungsoptionen und Lernpfaden im Rahmen von digitalen Schulungen, Präsenzschulungen, AWS Schulungspartnern und Zertifizierungen. Weitere Informationen finden Sie unter AWS Schulung und Zertifizierung.

AWS bietet sowohl kostenlose als auch abonnementbasierte Schulungen an, die mehrere Personen und Schwerpunktbereiche unterstützen. Besuchen Sie AWS Skillbuilder, um mehr zu erfahren.

Verstehe deine Umgebung AWS

Neben dem Verständnis von AWS Services, ihren Anwendungsfällen und ihrer Integration ist es ebenso wichtig zu verstehen, wie die AWS Umgebung Ihres Unternehmens tatsächlich aufgebaut ist und welche betrieblichen Prozesse vorhanden sind. Oft ist internes Wissen wie dieses nicht dokumentiert und wird nur von wenigen Fachexperten verstanden. Dies kann zu Abhängigkeiten führen, Innovationen behindern und die Reaktionszeit verlangsamen.

Um diese Abhängigkeiten zu vermeiden und die Reaktionszeiten zu verkürzen, sollte das interne Wissen über Ihre AWS Umgebung dokumentiert, zugänglich und für Ihre Sicherheitsanalysten verständlich sein. Um Ihren gesamten Cloud-Footprint zu verstehen, ist die Zusammenarbeit zwischen relevanten Sicherheitsakteuren und Cloud-Administratoren erforderlich. Ein Teil der Vorbereitung Ihrer Prozesse für die Reaktion auf Vorfälle umfasst die Dokumentation und Zentralisierung von Architekturdiagrammen, was the section called “Dokumentieren und zentralisieren Sie Architekturdiagramme” später in diesem Whitepaper behandelt wird. Aus Sicht der Mitarbeiter ist es jedoch wichtig, dass Ihre Analysten auf die Diagramme und Betriebsprozesse in Ihrer Umgebung zugreifen und diese verstehen können. AWS

Machen Sie sich mit AWS Reaktionsteams und Support vertraut

Support

Supportbietet eine Reihe von Tarifen, die Zugriff auf Tools und Fachwissen bieten, die den Erfolg und die Funktionsfähigkeit Ihrer AWS Lösungen unterstützen. Wenn Sie technischen Support und mehr Ressourcen für die Planung, Bereitstellung und Optimierung Ihrer AWS Umgebung benötigen, können Sie einen Supportplan wählen, der am besten zu Ihrem AWS Anwendungsfall passt.

Betrachten Sie das Support Center im AWS-Managementkonsole (Anmeldung erforderlich) als zentrale Anlaufstelle, um Support bei Problemen zu erhalten, die Ihre AWS Ressourcen betreffen. Der Zugriff auf Support wird von IAM gesteuert. Weitere Informationen zum Zugriff auf AWS Support-Funktionen finden Sie unter Erste Schritte mit Support.

Wenn Sie einen Missbrauch melden müssen, wenden Sie sich außerdem an das AWS Team für Vertrauen und Sicherheit.

Techniker für die Reaktion auf Sicherheitsvorfälle

Bei den Security Incident Response-Technikern handelt es sich um ein spezialisiertes, stets verfügbares globales AWS Team, das Kunden im Rahmen des Modells der AWS gemeinsamen Verantwortung bei aktiven Sicherheitsvorfällen unterstützt.

Wenn Sie von unseren Security Incident Response-Technikern unterstützt werden, erhalten Sie Unterstützung bei der Suche und Wiederherstellung eines aktiven Sicherheitsvorfalls am AWS. Mithilfe von AWS Serviceprotokollen unterstützen sie Sie bei der Ursachenanalyse und geben Ihnen Empfehlungen für die Wiederherstellung. Sie bieten auch Sicherheitsempfehlungen und bewährte Verfahren, mit denen Sie future Sicherheitsereignisse vermeiden können.

AWS Kunden können sich im Rahmen eines AWS Supportfalls an die Techniker für die Reaktion auf Sicherheitsvorfälle wenden.

- Alle Kunden:
  1. Konto und Abrechnung
  2. Service: Konto
  3. Kategorie: Sicherheit
  4. Schweregrad: Allgemeine Frage

- Kunden mit Support Developer-Plänen:
  1. Konto und Abrechnung
  2. Service: Konto
  3. Kategorie: Sicherheit
  4. Schweregrad: Wichtige Frage

- Kunden mit Support Geschäftsplänen:
  1. Konto und Abrechnung
  2. Service: Konto
  3. Kategorie: Sicherheit
  4. Schweregrad: Dringende Frage, die sich auf das Geschäft auswirkt

- Kunden mit Support Enterprise-Tarifen:
  1. Konto und Abrechnung

2. Service: Konto
3. Kategorie: Sicherheit
4. Schweregrad: Kritische Frage zum Geschäftsrisiko

- Kunden mit AWS Security Incident Response Abonnements: Öffnen Sie die Security Incident Response-Konsole unter https://console.aws.amazon.com/security-ir/

DDoS Response-Support

AWS bietet AWS Shieldeinen verwalteten verteilten Denial-of-Service (DDoS) -Schutzdienst, der Webanwendungen schützt, auf denen ausgeführt wird. AWS AWS Shield bietet eine ständig aktive Erkennung und automatische Inline-Abwehrmaßnahmen, mit denen Ausfallzeiten und Latenz von Anwendungen minimiert werden können, sodass kein Eingreifen erforderlich ist, um vom S-Schutz Support zu profitieren. DDo Es gibt zwei Stufen AWS Shield: Shield Standard und Shield Advanced. Informationen zu den Unterschieden zwischen diesen beiden Stufen finden Sie in der Dokumentation zu den Shield-Funktionen.

AWS Managed Services (AMS)

AWS Managed Services(AMS) sorgt für die kontinuierliche Verwaltung Ihrer AWS Infrastruktur, sodass Sie sich auf Ihre Anwendungen konzentrieren können. AMS trägt durch eine Implementierung bewährter Methoden zur Verwaltung Ihrer Infrastruktur dazu bei, den Betriebsaufwand zu reduzieren und das Risiko zu senken. Außerdem automatisiert AMS häufige Aktivitäten wie Änderungsanforderungen, Überwachung, Patch-Verwaltung, Sicherheit sowie Backup-Services und bietet während der gesamten Lebensdauer Services zum Bereitstellen, Ausführen und Unterstützen Ihrer Infrastruktur.

AMS übernimmt die Verantwortung für den Einsatz einer Reihe von Sicherheitskontrollen und reagiert täglich als Erste auf Warnmeldungen. Wenn eine Warnung ausgelöst wird, folgt AMS einer Reihe automatisierter und manueller Standard-Playbooks, um eine konsistente Reaktion zu gewährleisten. Diese Playbooks werden den AMS-Kunden während des Onboardings zur Verfügung gestellt, damit sie eine Reaktion entwickeln und mit AMS abstimmen können.

Prozess

Die Entwicklung gründlicher und klar definierter Prozesse zur Reaktion auf Vorfälle ist der Schlüssel zu einem erfolgreichen und skalierbaren Programm zur Reaktion auf Vorfälle. Wenn ein Sicherheitsereignis eintritt, helfen Ihnen klare Schritte und Workflows dabei, rechtzeitig zu reagieren.

Möglicherweise verfügen Sie bereits über Prozesse zur Reaktion auf Vorfälle. Unabhängig von Ihrem aktuellen Status ist es wichtig, Ihre Prozesse zur Vorfallreaktion regelmäßig zu aktualisieren, zu wiederholen und zu testen.

Entwickeln und testen Sie einen Plan zur Reaktion auf Vorfälle

Das erste Dokument, das für die Reaktion auf Vorfälle entwickelt werden muss, ist der Plan zur Reaktion auf Vorfälle. Der Vorfallreaktionsplan ist als Grundlage für Ihr Vorfallreaktionsprogramm und Ihre Vorfallreaktionsstrategie konzipiert. Ein Notfallplan ist ein Dokument auf hoher Ebene, das in der Regel die folgenden Abschnitte umfasst:

- Überblick über das Incident-Response-Team — Beschreibt die Ziele und Funktionen des Incident-Response-Teams
- Rollen und Zuständigkeiten — Führt die Beteiligten für die Reaktion auf Vorfälle auf und beschreibt ihre Rollen, wenn ein Vorfall eintritt
- Ein Kommunikationsplan — Erläutert die Kontaktinformationen und die Art und Weise, wie Sie während eines Vorfalls kommunizieren werden

  Es hat sich bewährt, die out-of-band Kommunikation als Backup für die Kommunikation bei Zwischenfällen zu nutzen. Ein Beispiel für eine Anwendung, die einen sicheren out-of-band Kommunikationskanal bereitstellt, ist AWS Wickr.
- Phasen der Reaktion auf Vorfälle und zu ergreifende Maßnahmen — Führt die Phasen der Reaktion auf Vorfälle auf, z. B. Erkennung, Analyse, Beseitigung, Eindämmung und Wiederherstellung — einschließlich der in diesen Phasen zu ergreifenden Maßnahmen auf hoher Ebene
- Definitionen für Schweregrad und Priorisierung von Vorfällen — Erläutert, wie der Schweregrad eines Vorfalls klassifiziert wird, wie der Vorfall priorisiert wird und wie sich die Schweregraddefinitionen dann auf die Eskalationsverfahren auswirken

Diese Abschnitte sind zwar in Unternehmen verschiedener Größen und Branchen üblich, der Vorfallreaktionsplan ist jedoch für jede Organisation individuell. Sie müssen einen Plan zur Reaktion auf Vorfälle erstellen, der für Ihr Unternehmen am besten geeignet ist.

Dokumentieren und zentralisieren Sie Architekturdiagramme

Um schnell und präzise auf ein Sicherheitsereignis reagieren zu können, müssen Sie wissen, wie Ihre Systeme und Netzwerke aufgebaut sind. Das Verständnis dieser internen Muster ist nicht nur wichtig für die Reaktion auf Vorfälle, sondern auch für die Überprüfung der Konsistenz zwischen

den Anwendungen, auf denen die Muster basieren, gemäß bewährten Methoden. Sie sollten auch sicherstellen, dass diese Dokumentation auf dem neuesten Stand ist und regelmäßig gemäß neuen Architekturmustern aktualisiert wird. Sie sollten Dokumentationen und interne Repositorien entwickeln, in denen unter anderem folgende Elemente detailliert beschrieben werden:

- AWS Kontostruktur — Sie müssen wissen:
  - Wie viele AWS Konten haben Sie?
  - Wie sind diese AWS Konten organisiert?
  - Wer sind die Geschäftsinhaber der AWS Konten?
  - Verwenden Sie Service Control-Richtlinien (SCPs)? Falls ja, welche organisatorischen Leitplanken werden verwendet? SCPs
  - Beschränken Sie die Regionen und Dienste, die genutzt werden können?
  - Welche Unterschiede gibt es zwischen Geschäftsbereichen und Umgebungen (dev/test/prod)?
- AWS Servicemuster
  - Welche AWS Dienste nutzen Sie?
  - Was sind die am häufigsten genutzten AWS Dienste?
- Architekturmuster
  - Welche Cloud-Architekturen verwenden Sie?
- AWS Authentifizierungsmuster
  - Wie authentifizieren sich Ihre Entwickler normalerweise? AWS
  - Verwenden Sie IAM-Rollen oder Benutzer (oder beides)? Ist Ihre Authentifizierung mit einem Identity Provider (IdP) AWS verbunden?
  - Wie ordnen Sie eine IAM-Rolle oder einen IAM-Benutzer einem Mitarbeiter oder System zu?
  - Wie wird der Zugriff gesperrt, wenn jemand nicht mehr autorisiert ist?
- AWS Autorisierungsmuster
  - Welche IAM-Richtlinien verwenden Ihre Entwickler?
  - Verwenden Sie ressourcenbasierte Richtlinien?
- Protokollierung und Überwachung
  - Welche Protokollierungsquellen verwenden Sie und wo werden sie gespeichert?
  - Aggregieren Sie AWS CloudTrail Logs? Falls ja, wo werden sie gespeichert?
  - Wie fragt man CloudTrail Logs ab?
  - Haben Sie Amazon GuardDuty aktiviert?

  - Wie greifen Sie auf GuardDuty Ergebnisse zu (z. B. Konsole, Ticketsystem, SIEM)?
  - Werden Ergebnisse oder Ereignisse in einem SIEM zusammengefasst?
  - Werden Tickets automatisch erstellt?
  - Welche Tools stehen zur Verfügung, um Protokolle für eine Untersuchung zu analysieren?
- Netzwerktopologie
  - Wie sind Geräte, Endpunkte und Verbindungen in Ihrem Netzwerk physisch oder logisch angeordnet?
  - Wie verbindet sich Ihr Netzwerk mit? AWS
  - Wie wird der Netzwerkverkehr zwischen Umgebungen gefiltert?
- Externe Infrastruktur
  - Wie werden nach außen gerichtete Anwendungen bereitgestellt?
  - Welche AWS Ressourcen sind öffentlich zugänglich?
  - Welche AWS Konten enthalten Infrastrukturen, die nach außen gerichtet sind?
  - Welche DDo S- oder externe Filterung gibt es?

Die Dokumentation interner technischer Diagramme und Prozesse erleichtert den Incident-Response-Analysten die Arbeit und hilft ihnen, sich schnell das institutionelle Wissen anzueignen, um auf ein Sicherheitsereignis zu reagieren. Eine gründliche Dokumentation der internen technischen Prozesse vereinfacht nicht nur Sicherheitsuntersuchungen, sondern dient auch der Rationalisierung und Bewertung der Prozesse.

Entwickeln Sie Playbooks zur Reaktion auf Vorfälle

Ein wichtiger Teil der Vorbereitung Ihrer Prozesse zur Vorfallreaktion ist die Entwicklung von Playbooks. Playbooks für die Vorfallreaktion enthalten eine Reihe von präskriptiven Anleitungen und Schritten, die Sie befolgen müssen, wenn ein Sicherheitsereignis eintritt. Eine klare Struktur und klare Schritte vereinfachen die Reaktion und verringern die Wahrscheinlichkeit menschlicher Fehler.

Wofür sollten Playbooks erstellt werden

Playbooks sollten für Vorfallszenarien wie die folgenden erstellt werden:

- Erwartete Vorfälle — Playbooks sollten für Vorfälle erstellt werden, die Sie erwarten. Dazu gehören Bedrohungen wie Denial of Service (DoS), Ransomware und die Kompromittierung von Anmeldeinformationen.

- Bekannte Sicherheitsfeststellungen oder Sicherheitswarnungen — Playbooks sollten für Ihre bekannten Sicherheitsfeststellungen und -warnungen, wie z. B. Ergebnisse, erstellt werden. GuardDuty Möglicherweise erhalten Sie ein GuardDuty Ergebnis und denken: „Was nun?“ Um zu verhindern, dass ein GuardDuty Ergebnis falsch behandelt oder das Ergebnis ignoriert wird, sollten Sie für jedes potenzielle Ergebnis ein Playbook erstellen. GuardDuty Einige Einzelheiten und Anleitungen zur Problembehebung finden Sie in der Dokumentation. GuardDuty Es ist erwähnenswert, dass dies standardmäßig nicht aktiviert GuardDuty ist und Kosten verursacht. Weitere Einzelheiten dazu GuardDuty finden Sie in Anhang A: Definitionen der Cloud-Funktionen -the section called “Sichtbarkeit und Alarmierung”.

Was sollte in Playbooks enthalten sein

Playbooks sollten technische Schritte enthalten, die ein Sicherheitsanalyst ausführen muss, um einen potenziellen Sicherheitsvorfall angemessen zu untersuchen und darauf zu reagieren.

Zu den Elementen, die in ein Playbook aufgenommen werden sollten, gehören:

- Überblick über das Playbook — Auf welches Risiko- oder Vorfallszenario bezieht sich dieses Playbook? Was ist das Ziel des Playbooks?
- Voraussetzungen — Welche Protokolle und Erkennungsmechanismen sind für dieses Vorfallszenario erforderlich? Wie lautet die erwartete Benachrichtigung?
- Informationen für Interessengruppen — Wer ist beteiligt und wie lauten ihre Kontaktinformationen? Welche Aufgaben haben die einzelnen Stakeholder?
- Reaktionsschritte — Welche taktischen Schritte sollten in allen Phasen der Reaktion auf Vorfälle ergriffen werden? Welche Abfragen sollte ein Analyst ausführen? Welcher Code sollte ausgeführt werden, um das gewünschte Ergebnis zu erzielen?
  - Erkennen — Wie wird der Vorfall erkannt?
  - Analysieren — Wie wird der Umfang der Auswirkungen bestimmt?
  - Eindämmen — Wie wird der Vorfall isoliert, um den Umfang einzuschränken?
  - Ausrotten — Wie wird die Bedrohung aus der Umwelt entfernt?
  - Wiederherstellung — Wie wird das betroffene System oder die betroffene Ressource wieder in Betrieb genommen?
- Erwartete Ergebnisse — Was ist das erwartete Ergebnis des Playbooks, nachdem Abfragen und Code ausgeführt wurden?

Um die Konsistenz der Informationen in jedem Playbook zu überprüfen, kann es hilfreich sein, eine Playbook-Vorlage zu erstellen, die Sie in Ihren anderen Sicherheits-Playbooks verwenden können. Einige der zuvor aufgeführten Elemente, wie z. B. Informationen zu Interessengruppen, können von mehreren Playbooks gemeinsam genutzt werden. Wenn das der Fall ist, können Sie eine zentrale Dokumentation für diese Informationen erstellen, im Playbook darauf verweisen und dann die expliziten Unterschiede im Playbook auflisten. Auf diese Weise müssen Sie nicht dieselben Informationen in all Ihren einzelnen Playbooks aktualisieren. Indem Sie eine Vorlage erstellen und allgemeine oder gemeinsam genutzte Informationen in Playbooks identifizieren, können Sie die Entwicklung von Playbooks vereinfachen und beschleunigen. Schließlich werden sich Ihre Playbooks wahrscheinlich im Laufe der Zeit weiterentwickeln. Sobald Sie sich vergewissert haben, dass die Schritte konsistent sind, bilden sich daraus die Voraussetzungen für die Automatisierung.

Beispiele für Playbooks

Eine Reihe von Beispiel-Playbooks finden Sie in Anhang B unter. the section called “Ressourcen für Playbooks” Anhand der hier aufgeführten Beispiele können Sie erfahren, welche Playbooks Sie erstellen und was Sie in Ihre Playbooks aufnehmen sollten. Es ist jedoch wichtig, dass Sie Playbooks erstellen, die die Risiken berücksichtigen, die für Ihr Unternehmen am relevantesten sind. Sie müssen sicherstellen, dass die Schritte und Workflows in Ihren Playbooks Ihre Technologien und Prozesse beinhalten.

Führen Sie regelmäßige Simulationen durch

Organizations wachsen und entwickeln sich im Laufe der Zeit, ebenso wie die Bedrohungslandschaft. Aus diesem Grund ist es wichtig, Ihre Fähigkeiten zur Reaktion auf Vorfälle kontinuierlich zu überprüfen. Simulationen sind eine Methode, mit der diese Bewertung durchgeführt werden kann. Simulationen verwenden reale Szenarien für Sicherheitsereignisse, die darauf ausgelegt sind, die Taktiken, Techniken und Verfahren eines Bedrohungsakteurs nachzuahmen (TTPs) und es einem Unternehmen zu ermöglichen, seine Fähigkeiten zur Reaktion auf Vorfälle zu testen und zu bewerten, indem es auf diese simulierten Cyberereignisse so reagiert, wie sie in der Realität auftreten könnten.

Simulationen bieten eine Vielzahl von Vorteilen, darunter:

- Validierung der Cybersicherheit und Stärkung des Vertrauens Ihres Vorfallreaktionsteams
- Testen der Genauigkeit und Effizienz von Tools und Workflows
- Optimierung der Kommunikations- und Eskalationsmethoden Ihres Vorfallreaktionsplans
- Möglichkeit, auf weniger verbreitete Vektoren zu reagieren

Arten von Simulationen

Es gibt drei Hauptarten von Simulationen:

- Übungen am Tisch — Beim Tabletop-Ansatz für Simulationen handelt es sich ausschließlich um eine Diskussionsrunde, an der die verschiedenen Akteure der Incident-Response teilnehmen, um Rollen und Verantwortlichkeiten zu üben und etablierte Kommunikationsinstrumente und Playbooks zu nutzen. Die Durchführung von Übungen kann in der Regel an einem ganzen Tag an einem virtuellen Ort, einem physischen Ort oder einer Kombination aus beidem durchgeführt werden. Aufgrund des Diskussionscharakters stehen bei der Tabletop-Übung Prozesse, Menschen und Zusammenarbeit im Mittelpunkt. Technologie ist ein integraler Bestandteil der Diskussion; der tatsächliche Einsatz von Tools oder Skripten zur Reaktion auf Vorfälle ist jedoch in der Regel nicht Teil der Übung am Tisch.
- Purple Team-Übungen — Purple Team-Übungen erhöhen den Grad der Zusammenarbeit zwischen den Incident-Respondern (Blue Team) und den simulierten Bedrohungsakteuren (Red Team). Das Blue Team besteht in der Regel aus Mitgliedern des Security Operations Center (SOC), kann aber auch andere Interessengruppen einbeziehen, die während eines tatsächlichen Cyberereignisses beteiligt wären. Das Red Team besteht in der Regel aus einem Penetrationstest-Team oder wichtigen Stakeholdern, die in offensiver Sicherheit geschult sind. Das Red Team arbeitet bei der Entwicklung eines Szenarios mit den Übungsleitern zusammen, damit das Szenario korrekt und durchführbar ist. Bei den Übungen von Purple Team liegt das Hauptaugenmerk auf den Erkennungsmechanismen, den Tools und den Standardarbeitsanweisungen (SOPs), die die Maßnahmen zur Reaktion auf Vorfälle unterstützen.
- Red Team-Übungen — Während einer Red Team-Übung führt die Offensive (Rotes Team) eine Simulation durch, um ein bestimmtes Ziel oder eine Reihe von Zielen innerhalb eines vorher festgelegten Umfangs zu erreichen. Die Verteidiger (blaues Team) kennen nicht unbedingt den Umfang und die Dauer der Übung, sodass sie realistischer einschätzen können, wie sie auf einen tatsächlichen Vorfall reagieren würden. Da es sich bei den Übungen des Roten Teams um invasive Tests handeln kann, sollten Sie vorsichtig sein und Kontrollen durchführen, um sicherzustellen, dass die Übung Ihrer Umgebung nicht tatsächlich schadet.

> **Note**
>
> AWS verlangt von Kunden, dass sie die auf der Penetrationstest-Website verfügbaren Richtlinien für Penetrationstests lesen, bevor sie Purple Team- oder Red Team-Übungen durchführen.

In Tabelle 1 sind einige wichtige Unterschiede zwischen diesen Simulationstypen zusammengefasst. Es ist wichtig zu beachten, dass die Definitionen im Allgemeinen als lose Definitionen betrachtet werden und an die Bedürfnisse Ihres Unternehmens angepasst werden können.

Tabelle 1 — Arten von Simulationen

	Übung am Tisch	Team-Übung in Violett	Rote Teamübung
Zusammenfassung	Übungen auf Papier, die sich auf ein bestimmtes Sicherheitsvorfallszenario konzentrieren. Diese können entweder anspruchsvoller oder technischer Natur sein und werden durch eine Reihe von Papiereinschüssen angetrieben.	Ein realistischeres Angebot im Vergleich zu Tischübungen. Bei den Purple Team-Übungen arbeiten die Moderatoren mit den Teilnehmern zusammen, um das Übungsengagement zu erhöhen und bei Bedarf Schulungen anzubieten.	Im Allgemeinen ein fortgeschritteneres Simulationsangebot. In der Regel besteht ein hohes Maß an Verdecktheit, sodass die Teilnehmer möglicherweise nicht alle Einzelheiten der Übung kennen.
Erforderliche Ressourcen	Begrenzte technische Ressourcen erforderlich	Verschiedene Interessengruppen erforderlich und ein hohes Maß an technischen Ressourcen erforderlich	Verschiedene Interessengruppen waren erforderlich und es wurden umfangreiche technische Ressourcen benötigt
Komplexität	Niedrig	Medium	Hoch

Erwägen Sie, in regelmäßigen Abständen Cybersimulationen durchzuführen. Jeder Übungstyp kann den Teilnehmern und der Organisation als Ganzes einzigartige Vorteile bieten. Sie können sich also dafür entscheiden, mit weniger komplexen Simulationstypen (wie Tischübungen) zu beginnen und zu komplexeren Simulationstypen (Red Team-Übungen) überzugehen. Wählen Sie auf der Grundlage Ihres Sicherheitsreifegrads, Ihrer Ressourcen und der gewünschten Ergebnisse einen Simulationstyp

aus. Einige Kunden entscheiden sich aufgrund der Komplexität und der Kosten möglicherweise nicht für die Durchführung von Red Team-Übungen.

Lebenszyklus des Trainings

Unabhängig von der Art der Simulation, die Sie wählen, folgen Simulationen im Allgemeinen diesen Schritten:

1. Definieren Sie die wichtigsten Übungselemente — Definieren Sie das Simulationsszenario und die Ziele der Simulation. Beide sollten von der Führungsebene akzeptiert werden.
2. Identifizieren Sie die wichtigsten Interessengruppen — Für eine Übung sind mindestens Übungsleiter und Teilnehmer erforderlich. Je nach Szenario können gegebenenfalls weitere Stakeholder einbezogen werden – etwa aus der Rechts- oder Kommunikationsabteilung oder aus der Geschäftsleitung.
3. Erstellen und testen Sie das Szenario — Das Szenario muss möglicherweise während der Erstellung neu definiert werden, wenn bestimmte Elemente nicht durchführbar sind. Als Ergebnis dieser Phase wird ein fertiges Szenario erwartet.
4. Erleichterung der Simulation — Die Art der Simulation bestimmt die verwendete Moderation (papiergestütztes Szenario im Vergleich zu einem hochtechnischen, simulierten Szenario). Die Übungsleiter sollten ihre Taktiken an den Übungsobjekten ausrichten und alle Übungsteilnehmer nach Möglichkeit einbeziehen, um den größtmöglichen Nutzen zu erzielen.
5. Entwickeln Sie den After Action Report (AAR) — Identifizieren Sie Bereiche, die gut gelaufen sind, Bereiche, die verbessert werden können, und mögliche Lücken. Der AAR sollte die Effektivität der Simulation sowie die Reaktion des Teams auf das simulierte Ereignis messen, damit der Fortschritt im Laufe der Zeit mit zukünftigen Simulationen verfolgt werden kann.

Technologie

Wenn Sie die entsprechenden Technologien vor einem Sicherheitsvorfall entwickeln und implementieren, können Ihre Mitarbeiter für die Reaktion auf Sicherheitsvorfälle diese untersuchen, den Umfang verstehen und rechtzeitig Maßnahmen ergreifen.

Entwickeln AWS Sie die Kontostruktur

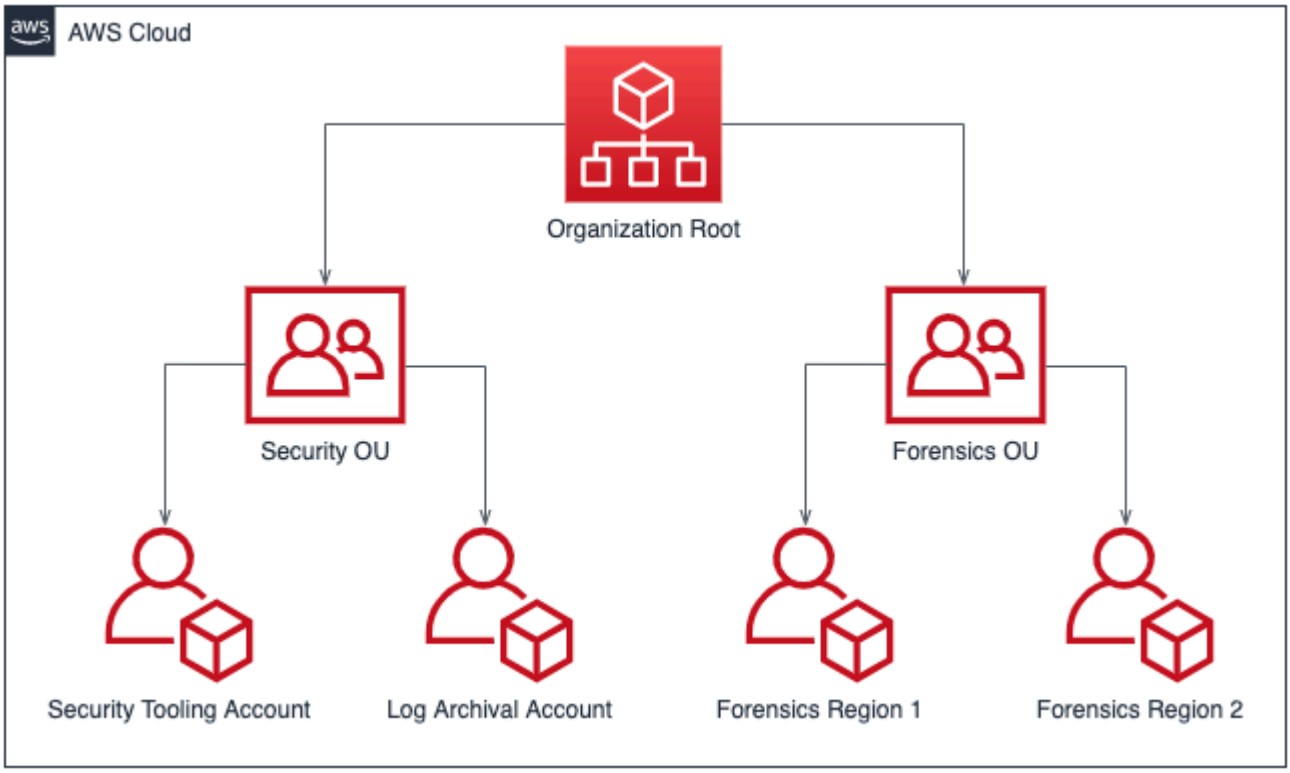
AWS Organizationshilft Ihnen dabei, eine AWS Umgebung zentral zu verwalten und zu steuern, während Sie Ihre AWS Ressourcen erweitern und skalieren. Eine AWS Organisation konsolidiert Ihre AWS Konten, sodass Sie sie als eine Einheit verwalten können. Sie können Organisationseinheiten (OUs) verwenden, um Konten zu gruppieren und sie als eine einzige Einheit zu verwalten.

Für die Reaktion auf Vorfälle ist es hilfreich, über eine AWS Kontostruktur zu verfügen, die die Funktionen der Incident-Response unterstützt. Dazu gehören eine Sicherheits-OU und eine Forensik-OU. Innerhalb der sicherheitsbezogenen Organisationseinheit sollten Sie über Konten für Folgendes verfügen:

- Protokollarchivierung — Aggregieren Sie die Protokolle in einem Protokollarchivierungskonto. AWS
- Sicherheitstools — Zentralisieren Sie Sicherheitsdienste in einem Sicherheitstool-Konto. AWS Dieses Konto fungiert als delegierter Administrator für Sicherheits-Services.

Innerhalb der forensischen Organisationseinheit haben Sie die Möglichkeit, für jede Region, in der Sie tätig sind, eines oder mehrere forensische Konten zu implementieren, je nachdem, was für Ihr Geschäfts- und Betriebsmodell am besten geeignet ist. Ein Beispiel für einen regionsspezifischen Kontoansatz: Wenn Sie nur in USA Ost (Nord-Virginia) (us-east-1) und US West (Oregon) (us-west-2) tätig sind, hätten Sie zwei Konten in der Forensik-OU: eines für us-east-1 und eines für us-west-2. Da die Bereitstellung neuer Konten etwas dauert, ist es unerlässlich, die forensischen Konten rechtzeitig vor einem Vorfall einzurichten und zu instrumentieren, damit die Notfallteams vorbereitet sind und sie effektiv nutzen können.

Das folgende Diagramm zeigt eine Beispiel-Kontenstruktur mit einer forensischen Organisationseinheit mit regionsspezifischen forensischen Konten:



Kontostruktur pro Region für die Reaktion auf Vorfälle

Entwickeln und Implementieren einer Markierungsstrategie

Es kann schwierig sein, Kontextinformationen zum geschäftlichen Anwendungsfall und zu relevanten internen Stakeholdern rund um eine AWS Ressource zu erhalten. Eine Möglichkeit, dies zu tun, sind Tags, die Ihren AWS Ressourcen Metadaten zuweisen und aus einem benutzerdefinierten Schlüssel und Wert bestehen. Sie können Tags erstellen, um Ressourcen nach Zweck, Besitzer, Umgebung, Art der verarbeiteten Daten und anderen Kriterien Ihrer Wahl zu kategorisieren.

Mit einer konsistenten Tagging-Strategie können Sie die Reaktionszeiten verkürzen, da Sie kontextbezogene Informationen zu einer Ressource schnell identifizieren und erkennen können. AWS Tags können auch als Mechanismus zur Initiierung von Reaktionsautomatisierungen dienen. Weitere Informationen darüber, was Sie taggen sollten, finden Sie in der Dokumentation zum Markieren von Ressourcen. AWS Sie sollten zunächst die Tags definieren, die Sie in Ihrer Organisation implementieren möchten. Anschließend können Sie diese Markierungsstrategie implementieren und erzwingen. Einzelheiten zur Implementierung und Durchsetzung finden Sie im AWS Blog Implementieren einer Strategie zur Kennzeichnung von AWS Ressourcen mithilfe von AWS Tag-Richtlinien und Dienststeuerungsrichtlinien () SCPs.

Kontaktinformationen für AWS das Konto aktualisieren

Für jedes Ihrer AWS Konten ist es wichtig, genaue up-to-date Kontaktinformationen zu haben, damit die richtigen Stakeholder wichtige Benachrichtigungen zu AWS Themen wie Sicherheit, Abrechnung und Betrieb erhalten. Für jedes AWS Konto haben Sie einen Hauptansprechpartner und alternative Ansprechpartner für Sicherheit, Abrechnung und Betrieb. Die Unterschiede zwischen diesen Kontakten finden Sie im Referenzhandbuch zur AWS Kontoverwaltung.

Einzelheiten zur Verwaltung alternativer Kontakte finden Sie in der AWS Dokumentation zum Hinzufügen, Ändern oder Entfernen alternativer Kontakte. Es hat sich bewährt, eine E-Mail-Verteilerliste zu verwenden, wenn Ihr Team sich um Abrechnungs-, Betriebs- und Sicherheitsprobleme kümmert. Eine E-Mail-Verteilerliste beseitigt Abhängigkeiten von einer Person, was zu Blockaden führen kann, wenn diese Person nicht im Büro ist oder das Unternehmen verlässt. Sie sollten auch sicherstellen, dass die E-Mail-Adresse und die Kontokontaktinformationen, einschließlich der Telefonnummer, gut geschützt sind, um sich vor Passwortrücksetzungen für Root-Konten und Zurücksetzungen der Multi-Faktor-Authentifizierung (MFA) zu schützen.

Für Kunden, die dies nutzen AWS Organizations, können Unternehmensadministratoren alternative Kontakte für Mitgliedskonten mithilfe des Verwaltungskontos oder eines delegierten Administratorkontos zentral verwalten, ohne dass für jedes Konto Anmeldeinformationen

erforderlich sind. AWS Sie müssen außerdem überprüfen, ob neu erstellte Konten über korrekte Kontaktinformationen verfügen. Informationen zum neu erstellten AWS-Konten Blogbeitrag finden Sie unter Alternative Kontakte automatisch aktualisieren.

Bereiten Sie den Zugriff auf vor AWS-Konten

Während eines Vorfalls müssen Ihre Incident-Response-Teams Zugriff auf die Umgebungen und Ressourcen haben, die an dem Vorfall beteiligt waren. Stellen Sie sicher, dass Ihre Teams über angemessenen Zugang verfügen, um ihre Aufgaben zu erfüllen, bevor ein Ereignis eintritt. Zu diesem Zweck sollten Sie wissen, welche Zugriffsebene Ihre Teammitglieder benötigen (z. B. welche Maßnahmen sie wahrscheinlich ergreifen werden), und im Voraus den Zugriff mit den geringsten Rechten einrichten.

Um diesen Zugriff zu implementieren und bereitzustellen, sollten Sie die AWS Kontostrategie und die Cloud-Identitätsstrategie mit den Cloud-Architekten Ihres Unternehmens festlegen und besprechen, um zu verstehen, welche Authentifizierungs- und Autorisierungsmethoden konfiguriert sind. Aufgrund des privilegierten Charakters dieser Anmeldeinformationen sollten Sie im Rahmen Ihrer Implementierung die Verwendung von Genehmigungsabläufen oder das Abrufen von Anmeldeinformationen aus einem Tresor oder Safe in Betracht ziehen. Nach der Implementierung sollten Sie den Zugriff der Teammitglieder dokumentieren und testen, lange bevor ein Ereignis eintritt, um sicherzustellen, dass sie ohne Verzögerungen reagieren können.

Und schließlich verfügen Benutzer, die speziell für die Reaktion auf einen Sicherheitsvorfall geschaffen wurden, häufig über Privilegien, um ausreichend Zugriff zu gewähren. Daher sollte die Verwendung dieser Anmeldeinformationen eingeschränkt, überwacht und nicht für alltägliche Aktivitäten verwendet werden.

Verstehen Sie die Bedrohungslandschaft

Entwickeln Sie Bedrohungsmodelle

Durch die Entwicklung von Bedrohungsmodellen können Unternehmen Bedrohungen und Abhilfemaßnahmen erkennen, bevor es ein nicht autorisierter Benutzer kann. Es gibt eine Reihe von Strategien und Ansätzen zur Bedrohungsmodellierung. Weitere Informationen finden Sie im Blogbeitrag How to Approach Threat Modeling. Bei der Reaktion auf Vorfälle kann ein Bedrohungsmodell dabei helfen, die Angriffsvektoren zu identifizieren, die ein Bedrohungsakteur während eines Vorfalls möglicherweise genutzt hat. Um rechtzeitig reagieren zu können, wird es entscheidend sein, zu verstehen, wovor Sie sich schützen. Sie können eine auch AWS Partner zur Bedrohungsmodellierung verwenden. Um nach einem AWS Partner zu suchen, verwenden Sie den AWS Partner Network.

Integrieren und nutzen Sie Informationen zu Cyberbedrohungen

Cyber-Bedrohungsinformationen sind Daten und Analysen zu den Absichten, Möglichkeiten und Fähigkeiten eines Bedrohungsakteurs. Die Beschaffung und Nutzung von Bedrohungsinformationen ist hilfreich, um einen Vorfall frühzeitig zu erkennen und das Verhalten von Bedrohungsakteuren besser zu verstehen. Zu den Informationen über Cyberbedrohungen gehören statische Indikatoren wie IP-Adressen oder Datei-Hashes von Malware. Dazu gehören auch allgemeine Informationen wie Verhaltensmuster und Absichten. Sie können Bedrohungsinformationen von einer Reihe von Anbietern von Cybersicherheit und aus Open-Source-Repositorys sammeln.

Um Bedrohungsinformationen für Ihre AWS Umgebung zu integrieren und zu maximieren, können Sie einige out-of-the-box Funktionen nutzen und Ihre eigenen Threat-Intelligence-Listen integrieren. Amazon GuardDuty verwendet AWS interne und externe Quellen für Bedrohungsinformationen. Andere AWS Dienste, wie eine DNS-Firewall und AWS WAF Regeln, nehmen ebenfalls Eingaben von der Gruppe AWS„Advanced Threat Intelligence“ entgegen. Einige GuardDuty Ergebnisse sind dem MITRE ATT&CK Framework zugeordnet, das Informationen über reale Beobachtungen zu Taktiken und Techniken von Gegnern bereitstellt.

Auswählen und Einrichten von Protokollen für die Analyse und Alarmierung

Bei einer Sicherheitsuntersuchung müssen Sie relevante Protokolle heranziehen können, um alle Aspekte und den Zeitrahmen des Vorfalls zu verstehen. Protokolle werden auch für die Generierung von Warnungen benötigt, die auf bestimmte Ereignisse aufmerksam machen. Es ist sehr wichtig, Abfrage- und Abrufmechanismen auszuwählen, zu aktivieren, zu speichern und einzurichten sowie die Alarmierung einzurichten. Jede dieser Aktionen wird in diesem Abschnitt besprochen. Weitere Informationen finden Sie im AWS Blogbeitrag Protokollierungsstrategien für die Reaktion auf Sicherheitsvorfälle.

Wählen und aktivieren Sie Protokollquellen

Im Vorfeld einer Sicherheitsuntersuchung müssen Sie relevante Protokolle erfassen, um die Aktivitäten in einem AWS Konto rückwirkend rekonstruieren zu können. Wählen und aktivieren Sie Protokollquellen, die für die Workloads ihrer AWS Konten relevant sind.

AWS CloudTrail ist ein Protokollierungsdienst, der API-Aufrufe im Zusammenhang mit einer AWS AWS Kontoerfassungsdienstaktivität verfolgt. Er ist standardmäßig aktiviert und ermöglicht die 90-tägige Aufbewahrung von Verwaltungsereignissen, die über CloudTrail die Funktion „Event History“ mit AWS-Managementkonsole dem AWS CLI oder einem AWS SDK abgerufen werden können. Für eine längere Aufbewahrung und Sichtbarkeit von Datenereignissen müssen Sie einen CloudTrail Trail erstellen und ihn einem Amazon S3 S3-Bucket und optional einer CloudWatch Protokollgruppe

zuordnen. Alternativ können Sie einen CloudTrail Lake erstellen, der CloudTrail Protokolle für bis zu sieben Jahre aufbewahrt und eine SQL-basierte Abfragefunktion bietet.

AWS empfiehlt Kunden, die eine VPC verwenden, Netzwerkverkehr und DNS-Protokolle mithilfe von VPC Flow Logs bzw. Amazon Route 53 Resolver-Abfrageprotokollen zu aktivieren und diese entweder in einen Amazon S3 S3-Bucket oder eine CloudWatch Protokollgruppe zu streamen. Sie können ein VPC-Flow-Protokoll für eine VPC, ein Subnetz oder eine Netzwerkschnittstelle erstellen. Bei VPC Flow Logs können Sie auswählen, wie und wo Sie Flow Logs aktivieren, um die Kosten zu senken.

AWS CloudTrail Protokolle, VPC-Flow-Logs und Route 53-Resolver-Abfrageprotokolle sind die grundlegenden Protokollierungs-Trifecta zur Unterstützung von Sicherheitsuntersuchungen. AWS

AWS Services können Protokolle generieren, die nicht von den grundlegenden Protokollierungs-Trifecta erfasst werden, wie z. B. Elastic Load Balancing Balancing-Logs, AWS WAF Logs, AWS Config Recorder-Logs, GuardDuty Amazon-Ergebnisse, Amazon Elastic Kubernetes Service (Amazon EKS) Audit-Logs und Amazon EC2 EC2-Instance-Betriebssystem- und Anwendungsprotokolle. Die vollständige Liste der the section called “Anhang A: Definitionen der Cloud-Funktionen” Protokollierungs- und Überwachungsoptionen finden Sie unter.

Wählen Sie Protokollspeicher

Die Wahl des Protokollspeichers hängt im Allgemeinen vom verwendeten Abfragetool, den Aufbewahrungsmöglichkeiten, der Vertrautheit und den Kosten ab. Wenn Sie AWS Serviceprotokolle aktivieren, stellen Sie eine Speichereinrichtung bereit, normalerweise einen Amazon S3 S3-Bucket oder eine CloudWatch Protokollgruppe.

Ein Amazon S3 S3-Bucket bietet kostengünstigen, dauerhaften Speicher mit einer optionalen Lebenszyklusrichtlinie. In Amazon S3 S3-Buckets gespeicherte Protokolle können mithilfe von Diensten wie Amazon Athena nativ abgefragt werden. Eine CloudWatch Protokollgruppe bietet dauerhaften Speicherplatz und eine integrierte Abfragefunktion über Logs Insights. CloudWatch

Identifizieren Sie die geeignete Protokollaufbewahrung

Wenn Sie einen S3-Bucket oder eine CloudWatch S3-Protokollgruppe zum Speichern von Protokollen verwenden, müssen Sie für jede Protokollquelle angemessene Lebenszyklen einrichten, um die Speicher- und Abrufkosten zu optimieren. Kunden stehen in der Regel zwischen 3 und 12 Monaten an Protokollen für Abfragen zur Verfügung, die bis zu sieben Jahre aufbewahrt werden können. Die Wahl von Verfügbarkeit und Aufbewahrungszeit sollte sich nach Ihren Sicherheitsanforderungen und einer Kombination aus gesetzlichen, regulatorischen und unternehmensinternen Vorschriften richten.

Wählen und implementieren Sie Abfragemechanismen für Protokolle

Die wichtigsten Dienste AWS, mit denen Sie Protokolle abfragen können, sind CloudWatch Logs Insights für in CloudWatch Protokollgruppen gespeicherte Daten sowie Amazon Athena und Amazon OpenSearch Service für in Amazon S3 gespeicherte Daten. Sie können auch Abfragetools von Drittanbietern wie SIEM (Security Information and Event Management) verwenden.

Bei der Auswahl eines Tools zur Protokollabfrage sollten Sie die Personen, die Prozesse und die Technologieaspekte Ihrer Sicherheitsoperationen berücksichtigen. Wählen Sie ein Tool, das betriebliche, geschäftliche und Sicherheitsanforderungen erfüllt und sowohl zugänglich als auch langfristig wartbar ist. Denken Sie daran, dass Tools zur Protokollabfrage optimal funktionieren, wenn die Anzahl der zu durchsuchenden Protokolle im Rahmen der Limits des jeweiligen Tools liegt. Es ist nicht ungewöhnlich, dass Kunden aus Kosten- oder technischen Gründen über mehrere Abfragetools verfügen. Beispielsweise könnten Kunden ein SIEM eines Drittanbieters verwenden, um Abfragen für die Daten der letzten 90 Tage durchzuführen, und Athena verwenden, um Abfragen über 90 Tage hinaus durchzuführen, da ein SIEM die Protokollaufnahme kostet. Stellen Sie unabhängig von der Implementierung sicher, dass Ihr Ansatz die Anzahl der Tools minimiert, die zur Maximierung der betrieblichen Effizienz erforderlich sind, insbesondere bei der Untersuchung eines Sicherheitsvorfalls.

Verwenden Sie Protokolle für Warnmeldungen

AWS bietet nativ Benachrichtigungen über Sicherheitsdienste wie Amazon GuardDuty AWS Security Hub CSPM, und. AWS Config Sie können auch benutzerdefinierte Engines zur Generierung von Warnmeldungen für Sicherheitswarnungen verwenden, die nicht von diesen Diensten abgedeckt werden, oder für spezifische Warnmeldungen, die für Ihre Umgebung relevant sind. Die Erstellung dieser Warnmeldungen und Erkennungen wird in dem Abschnitt behandelt, der the section called “Erkennung” in diesem Dokument genannt wird.

Entwickeln Sie forensische Fähigkeiten

Bevor es zu einem Sicherheitsvorfall kommt, empfiehlt es sich gegebenenfalls, forensische Funktionen zur Unterstützung der Untersuchung von Sicherheitsereignissen zu entwickeln. Der Leitfaden zur Integration forensischer Techniken in die Reaktion auf Vorfälle von NIST bietet solche Anleitungen.

Forensik auf AWS

Konzepte aus der traditionellen Forensik vor Ort gelten für. AWS Die Strategien für forensische Ermittlungsumgebungen im AWS Cloud Blogbeitrag bieten Ihnen wichtige Informationen, auf die Sie bei der Migration ihrer forensischen Expertise zurückgreifen können. AWS

Sobald Sie Ihre Umgebung und AWS Kontostruktur für die Forensik eingerichtet haben, sollten Sie die Technologien definieren, die für die effektive Durchführung forensisch fundierter Methoden in den vier Phasen erforderlich sind:

- Erfassung — Sammeln Sie relevante AWS Protokolle AWS CloudTrail AWS Config, wie VPC Flow Logs und Logs auf Hostebene. Sammeln Sie Snapshots, Backups und Speicherabbilder der betroffenen Ressourcen. AWS
- Untersuchung — Untersuchen Sie die gesammelten Daten, indem Sie die relevanten Informationen extrahieren und auswerten.
- Analyse — Analysieren Sie die gesammelten Daten, um den Vorfall zu verstehen und daraus Schlüsse zu ziehen.
- Berichterstattung — Präsentieren Sie die Informationen, die sich aus der Analysephase ergeben.

Erfassen von Backups und Snapshots

Die Einrichtung von Backups wichtiger Systeme und Datenbanken ist für die Wiederherstellung nach einem Sicherheitsvorfall und für forensische Zwecke von entscheidender Bedeutung. Mit vorhandenen Backups können Sie Ihre Systeme wieder in einen vorherigen sicheren Zustand versetzen. Mit dieser AWS Option können Sie Schnappschüsse verschiedener Ressourcen erstellen. Mit Snapshots erhalten Sie point-in-time Backups dieser Ressourcen. Es gibt viele AWS -Services, die Sie beim Backup und der Wiederherstellung unterstützen können. Einzelheiten zu diesen Services und Ansätzen für Backup und Recovery finden Sie in den Backup and Recovery Prescriptive Guidance. Weitere Informationen finden Sie im Blogbeitrag Verwenden von Backups zur Wiederherstellung nach Sicherheitsvorfällen.

Vor allem, wenn es um Situationen wie Ransomware geht, ist es wichtig, dass Ihre Backups gut geschützt sind. Anleitungen zur Sicherung Ihrer Backups finden Sie in den 10 besten Sicherheitsmethoden für die Sicherung von Backups im AWS Blogbeitrag. Zusätzlich zum Schutz Ihrer Backups sollten Sie Ihre Backup- und Wiederherstellungsprozesse regelmäßig testen, um sicherzustellen, dass die vorhandenen Technologien und Prozesse wie erwartet funktionieren.

Automatisierung der Forensik auf AWS

Während eines Sicherheitsereignisses muss Ihr Incident-Response-Team in der Lage sein, schnell Beweise zu sammeln und zu analysieren und gleichzeitig die Genauigkeit für den Zeitraum, in dem das Ereignis stattfindet, zu gewährleisten. Für das Incident-Response-Team ist es sowohl schwierig als auch zeitaufwändig, die relevanten Beweise manuell in einer Cloud-Umgebung zu sammeln, insbesondere bei einer großen Anzahl von Instanzen und Konten. Darüber hinaus kann die manuelle

Erfassung anfällig für menschliche Fehler sein. Aus diesen Gründen sollten Kunden Automatisierung für die Forensik entwickeln und implementieren.

AWS bietet eine Reihe von Automatisierungsressourcen für die Forensik, die im Anhang unter zusammengefasst sind. the section called “Forensische Ressourcen” Diese Ressourcen sind Beispiele für forensische Muster, die von entwickelt und von Kunden implementiert wurden. Obwohl sie für den Anfang eine nützliche Referenzarchitektur sein können, sollten Sie erwägen, sie zu ändern oder neue forensische Automatisierungsmuster zu erstellen, die auf Ihrer Umgebung, Ihren Anforderungen, Tools und forensischen Prozessen basieren.

Zusammenfassung der vorbereitenden Punkte

Eine gründliche Vorbereitung der Reaktion auf Sicherheitsvorfälle ist entscheidend für eine zeitnahe und effektive Reaktion auf Vorfälle. Bei der Vorbereitung der Reaktion auf Vorfälle sind Mitarbeiter, Prozesse und Technologien involviert. Alle drei Bereiche sind für die Vorbereitung gleich wichtig. Sie sollten Ihr Incident-Response-Programm für alle drei Bereiche vorbereiten und weiterentwickeln.

In Tabelle 2 sind die in diesem Abschnitt aufgeführten Vorbereitungspunkte zusammengefasst.

Tabelle 2 — Punkte zur Vorbereitung der Reaktion auf Vorfälle

Domain	Gegenstand der Vorbereitung	Aktionselemente
Leute	Definieren Sie Rollen und Verantwortlichkeiten.	• Identifizieren Sie die für die Reaktion auf Vorfälle relevanten Akteure. • Entwickeln Sie ein Diagramm für einen Vorfall, der verantwortungsbewu sst, rechenschaftspflichtig, informiert und konsultiert wurde (RACI).
Menschen	Schulen Sie Mitarbeiter für die Reaktion auf Vorfälle darin AWS.	• Schulen Sie die Beteiligten bei der Reaktion auf Vorfälle auf AWS Fundamenten. • Schulen Sie die Akteure bei der Reaktion auf Vorfälle in

Domain	Gegenstand der Vorbereitung	Aktionselemente
		AWS Bezug auf Sicherheits- und Überwachungsdienste. • Informieren Sie die Beteiligten bei der Reaktion auf Vorfälle über Ihre AWS Umgebung und deren Architektur.
Menschen	Verstehen Sie AWS die Support-Optionen.	• Machen Sie sich mit den Unterschieden in Bezug auf AWS Support, Security Incident Response Engineers, DDo S Response Team (DRT) und AMS vertraut. • Machen Sie sich mit dem Weg zur Triage und Eskalation vertraut, um die Security Incident Response-Techniker bei Bedarf während eines aktiven Sicherheitsereignisses zu erreichen.
Prozess	Entwickeln Sie einen Plan zur Reaktion auf Vorfälle.	• Erstellen Sie ein Dokument auf hoher Ebene, das Ihr Programm und Ihre Strategie zur Reaktion auf Vorfälle definiert. • Nehmen Sie einen RACI, einen Kommunikationsplan , Definitionen von Vorfällen und Phasen der Reaktion auf Vorfälle in den Plan zur Reaktion auf Vorfälle auf.

Domain	Gegenstand der Vorbereitung	Aktionselemente
Prozess	Dokumentieren und zentralisieren Sie Architekturdiagramme.	• Dokumentieren Sie Einzelheiten zur Konfiguration Ihrer AWS Umgebung in Bezug auf Kontostruktur, Servicenutzung, IAM-Muster und andere Kernfunktionen Ihrer Konfiguration. AWS • Entwickeln Sie Architekturdiagramme Ihrer Cloud-Architekturen.
Prozess	Entwickeln Sie Playbooks zur Reaktion auf Vorfälle.	• Erstellen Sie eine Vorlage für die Struktur Ihrer Playbooks. • Erstellen Sie Playbooks für erwartete Sicherheitsereignisse. • Erstellen Sie Playbooks für bekannte Sicherheitswarnungen, wie z. B. GuardDuty Ergebnisse.
Prozess	Führen Sie regelmäßige Simulationen durch.	• Entwickeln Sie einen regelmäßigen Rhythmus, um Vorfallsimulationen durchzuführen. • Nutzen Sie die Ergebnisse und gewonnenen Erkenntnisse, um Ihr Programm zur Reaktion auf Vorfälle weiterzuentwickeln.

Domain	Gegenstand der Vorbereitung	Aktionselemente
Technologie	Entwickeln Sie eine AWS Kontostruktur.	• Planen Sie eine Kontostruktur, in der festgelegt ist, wie Workloads nach AWS Konten getrennt werden. • Erstellen Sie eine Sicherheits-OU mit einem Sicherheitstool und einem Konto für die Protokollarchivierung. • Erstellen Sie eine forensische Organisationseinheit mit forensischen Konten für jede Region, in der Sie tätig sind.
Technologie	Entwickeln und implementieren Sie eine Tagging-Strategie, die es den Einsatzkräften ermöglicht, die Verantwortung und den Kontext der Ergebnisse zu identifizieren.	• Planen Sie eine Strategie für das Tagging und welche Tags Sie mit Ihren Ressourcen verknüpfen möchten. AWS • Implementieren Sie die Tagging-Strategie und setzen Sie sie durch.

Domain	Gegenstand der Vorbereitung	Aktionselemente
Technologie	Kontaktinformationen für das AWS Konto aktualisieren.	• Vergewissern Sie sich, dass AWS für die Konten Kontaktinformationen aufgeführt sind. • Erstellen Sie E-Mail-Verteilerlisten für die Kontaktinformationen, um einzelne Fehlerquellen zu vermeiden. • Schützen Sie die E-Mail-Konten, die mit den AWS Kontoinformationen verknüpft sind.
Technologie	Bereiten Sie den Zugriff auf AWS Konten vor.	• Definieren Sie, welchen Zugriff Incident-Responder benötigen, um auf einen Vorfall zu reagieren. • Implementieren, testen und überwachen Sie den Zugriff.
Technologie	Verstehen Sie die Bedrohungslandschaft.	• Entwickeln Sie Bedrohungsmodelle für Ihre Umgebung und Anwendungen. • Integrieren und nutzen Sie Informationen zu Cyberbedrohungen.

Domain	Gegenstand der Vorbereitung	Aktionselemente
Technologie	Wählen Sie Protokolle aus und richten Sie sie ein.	• Identifizieren und aktivieren Sie Protokolle für Untersuchungen. • Wählen Sie Protokollspeicher aus. • Identifizieren und implementieren Sie die Protokollaufbewahrung. • Entwickeln Sie einen Mechanismus zum Abrufen und Abfragen von Protokollen und Artefakten. • Verwenden Sie Protokolle für Warnmeldungen.
Technologie	Entwickeln Sie forensische Fähigkeiten.	• Identifizieren Sie Artefakte, die für die forensische Erfassung erforderlich sind. • Erfassen und sichern Sie Backups wichtiger Systeme. • Definieren Sie Mechanismen für die Analyse identifizierter Logs und Artefakte. • Implementieren Sie Automatisierung für forensische Analysen.

Für die Vorbereitung der Reaktion auf Vorfälle wird ein iterativer Ansatz empfohlen. All diese Vorbereitungsschritte können nicht über Nacht erledigt werden. Sie sollten einen Plan erstellen, um klein anzufangen und Ihre Fähigkeiten zur Reaktion auf Vorfälle im Laufe der Zeit kontinuierlich zu verbessern.

Operationen

Der Betrieb ist der Kern der Reaktion auf Vorfälle. Hier finden die Maßnahmen zur Reaktion und Behebung von Sicherheitsvorfällen statt. Der Betrieb umfasst die folgenden fünf Phasen: Erkennung, Analyse, Eindämmung, Beseitigung und Wiederherstellung. Eine Beschreibung dieser Phasen und der Ziele finden Sie in Tabelle 3.

Tabelle 3 — Betriebsphasen

Phase	Ziel
Erkennung	Identifizieren eines potenziellen Sicherhei tsereignisses.
Analyse	Stellen Sie fest, ob es sich bei einem Sicherhei tsereignis um einen Vorfall handelt, und beurteilen Sie den Umfang des Vorfalls.
Eindämmung	Minimieren und Beschränken des Umfangs des Sicherheitsereignisses.
Ausrottung	Entfernen nicht autorisierter Ressourcen oder Artefakte im Zusammenhang mit dem Sicherhei tsereignis. Implementieren von Abhilfema ßnahmen zur Behebung der Ursache des Sicherheitsvorfalls.
Erholung	Stellen Sie die Systeme in einen bekannten sicheren Zustand zurück und überwachen Sie diese Systeme, um sicherzustellen, dass die Bedrohung nicht erneut auftritt.

Die Phasen sollen als Leitfaden für die Reaktion auf Sicherheitsvorfälle und deren Behandlung dienen, damit Sie effektiv und nachhaltig reagieren können. Die tatsächlichen Maßnahmen, die Sie ergreifen, sind abhängig vom jeweiligen Vorfall. Bei einem Vorfall mit Ransomware müssen beispielsweise andere Schritte ausgeführt werden als bei einem Vorfall, an dem ein öffentlicher Amazon-S3-Bucket beteiligt ist. Darüber hinaus folgen diese Phasen nicht unbedingt aufeinander.

Nach der Eindämmung und Beseitigung müssen Sie möglicherweise zur Analyse zurückkehren, um zu ermitteln, ob Ihre Maßnahmen wirksam waren.

Erkennung

Eine Warnung ist der Hauptbestandteil der Erkennungsphase. Sie generiert eine Benachrichtigung, um den Prozess zur Reaktion auf Vorfälle auf der Grundlage der relevanten Aktivität der AWS Kontobedrohung einzuleiten.

Die Genauigkeit von Warnmeldungen ist eine Herausforderung. Es ist nicht immer möglich, mit absoluter Sicherheit zu bestimmen, ob ein Vorfall eingetreten ist, im Gange ist oder ob er in future passieren wird. Hier sind ein paar Gründe:

- Erkennungsmechanismen basieren auf Basisabweichungen, bekannten Mustern und Benachrichtigungen von internen oder externen Stellen.
- Aufgrund der Unvorhersehbarkeit der Technologie und der Menschen bzw. der Mittel und Akteure von Sicherheitsvorfällen ändern sich die Ausgangswerte im Laufe der Zeit. Durch neuartige oder modifizierte Taktiken, Techniken und Verfahren der Bedrohungsakteure entstehen bösartige Muster (). TTPs
- Änderungen an Mitarbeitern, Technologien und Prozessen werden nicht sofort in den Prozess zur Reaktion auf Vorfälle integriert. Einige werden im Verlauf einer Untersuchung entdeckt.

Quellen der Warnung

Sie sollten erwägen, die folgenden Quellen zur Definition von Warnmeldungen zu verwenden:

- Ergebnisse — AWS Dienste wie Amazon GuardDuty, Amazon Macie AWS Security Hub CSPM, Amazon Inspector AWS Config, IAM Access Analyzer und Network Access Analyzer generieren Ergebnisse, die zur Erstellung von Warnmeldungen verwendet werden können.
- Protokolle — AWS Service-, Infrastruktur- und Anwendungsprotokolle, die in Amazon S3 S3-Buckets und CloudWatch Protokollgruppen gespeichert sind, können analysiert und korreliert werden, um Warnmeldungen zu generieren.
- Abrechnungsaktivität — Eine plötzliche Änderung der Abrechnungsaktivität kann auf ein Sicherheitsereignis hinweisen. Folgen Sie der Dokumentation unter Einrichtung eines Fakturierungsalarms zur Überwachung Ihrer geschätzten AWS Gebühren, um dies zu überprüfen.
- Informationen zu Cyberbedrohungen — Wenn Sie einen Feed mit Informationen zu Cyberbedrohungen eines Drittanbieters abonnieren, können Sie diese Informationen mit anderen

Protokollierungs- und Überwachungstools korrelieren, um potenzielle Indikatoren für Ereignisse zu identifizieren.

- Partner-Tools — Partner im AWS Partner Network (APN) bieten erstklassige Produkte, mit denen Sie Ihre Sicherheitsziele erreichen können. Bei der Reaktion auf Vorfälle können Partnerprodukte mit Endpoint Detection and Response (EDR) oder SIEM dabei helfen, Ihre Ziele bei der Reaktion auf Vorfälle zu unterstützen. Weitere Informationen finden Sie unter Sicherheitspartnerlösungen und Sicherheitslösungen im AWS Marketplace.
- AWS Vertrauen und Sicherheit — Wir Support könnten Kunden kontaktieren, wenn wir missbräuchliche oder böswillige Aktivitäten feststellen.
- Einmaliger Kontakt — Da es Ihre Kunden, Entwickler oder andere Mitarbeiter in Ihrem Unternehmen sein können, denen etwas Ungewöhnliches auffällt, ist es wichtig, dass Sie Ihr Sicherheitsteam über eine bekannte und gut bekannt gemachte Methode kontaktieren. Zu den beliebtesten Optionen gehören Ticketsysteme, Kontakt-E-Mail-Adressen und Webformulare. Wenn Ihre Organisation mit der breiten Öffentlichkeit zusammenarbeitet, benötigen Sie möglicherweise auch einen Sicherheitsmechanismus für die Öffentlichkeit.

Weitere Informationen zu Cloud-Funktionen, die Sie bei Ihren Untersuchungen nutzen können, finden Sie the section called “Anhang A: Definitionen der Cloud-Funktionen” in diesem Dokument.

Erkennung als Teil der Sicherheitskontrolltechnik

Erkennungsmechanismen sind ein integraler Bestandteil der Entwicklung der Sicherheitskontrolle. Sobald Richtlinien und präventive Kontrollen definiert sind, sollten entsprechende detektive und reaktive Kontrollen eingeführt werden. Beispielsweise richtet eine Organisation eine Direktive für den Root-Benutzer eines AWS Kontos ein, die nur für bestimmte und sehr genau definierte Aktivitäten verwendet werden sollte. Sie verbinden sie mit einer präventiven Kontrolle, die mithilfe der Service Control Policy (SCP) einer AWS Organisation implementiert wird. Wenn Root-Benutzeraktivitäten über den erwarteten Basiswert hinausgehen, wird das Security Operations Center (SOC) durch eine detektive Kontrolle, die mit einer EventBridge Regel und einem SNS-Thema implementiert wurde, benachrichtigt. Bei der Reaktionssteuerung wählt das SOC das passende Playbook aus, führt Analysen durch und arbeitet, bis der Vorfall behoben ist.

Sicherheitskontrollen lassen sich am besten anhand der Bedrohungsmodellierung der Workloads definieren, in denen sie ausgeführt werden. AWS Die Wichtigkeit detektiver Kontrollen wird anhand der Business Impact Analysis (BIA) für die jeweilige Arbeitslast festgelegt. Durch detektivische Kontrollen ausgelöste Warnmeldungen werden nicht unmittelbar nach ihrem Eingang behandelt, sondern auf der Grundlage ihrer anfänglichen Kritikalität, die im Laufe der Analyse angepasst

werden muss. Die Festlegung der anfänglichen Kritikalität dient als Hilfe bei der Priorisierung. Der Kontext, in dem die Warnung ausgelöst wurde, bestimmt ihre tatsächliche Kritikalität. Beispielsweise verwendet eine Organisation Amazon GuardDuty als Bestandteil der Detective Control, die für EC2-Instances verwendet wird, die Teil eines Workloads sind. Das Ergebnis `Impact:EC2/SuspiciousDomainRequest.Reputation` wird generiert und informiert Sie darüber, dass die aufgelistete Amazon EC2 EC2-Instance innerhalb Ihres Workloads einen Domainnamen abfragt, bei dem der Verdacht besteht, dass er bösartig ist. Diese Warnung ist standardmäßig auf einen niedrigen Schweregrad eingestellt. Im Verlauf der Analysephase wurde festgestellt, dass mehrere hundert EC2-Instances dieses Typs von einem nicht autorisierten Akteur bereitgestellt `p4d.24xlarge` wurden, was die Betriebskosten des Unternehmens erheblich in die Höhe trieb. Zu diesem Zeitpunkt trifft das Incident-Response-Team die Entscheidung, die Kritikalität dieser Warnung auf hoch zu setzen, wodurch das Gefühl der Dringlichkeit verstärkt und weitere Maßnahmen beschleunigt werden. Beachten Sie, dass der Schweregrad des GuardDuty Befundes nicht geändert werden kann.

Implementierungen von Detective Control

Es ist wichtig zu verstehen, wie Detective Controls implementiert werden, da sie dazu beitragen, zu bestimmen, wie die Warnung für ein bestimmtes Ereignis verwendet wird. Es gibt zwei Hauptimplementierungen von technischen Detektivkontrollen:

- Die Verhaltenserkennung basiert auf mathematischen Modellen, die allgemein als maschinelles Lernen (ML) oder künstliche Intelligenz (KI) bezeichnet werden. Die Erkennung erfolgt durch Inferenz. Daher spiegelt die Warnung möglicherweise nicht unbedingt ein aktuelles Ereignis wider.
- Die regelbasierte Erkennung ist deterministisch. Kunden können die genauen Parameter dafür festlegen, bei welcher Aktivität gewarnt werden soll, und das ist sicher.

Moderne Implementierungen von Erkennungssystemen, wie z. B. ein Intrusion Detection System (IDS), verfügen in der Regel über beide Mechanismen. Im Folgenden finden Sie einige Beispiele für regelbasierte und verhaltensbasierte Erkennungen mit. GuardDuty

- Wenn das Ergebnis generiert `Exfiltration:IAMUser/AnomalousBehavior` wird, werden Sie darüber informiert, dass „in Ihrem Konto eine ungewöhnliche API-Anfrage festgestellt wurde“. Wenn Sie sich die Dokumentation genauer ansehen, erfahren Sie, dass „das ML-Modell alle API-Anfragen in Ihrem Konto auswertet und ungewöhnliche Ereignisse identifiziert, die mit den von Gegnern verwendeten Techniken in Verbindung stehen“, was darauf hindeutet, dass es sich bei diesem Befund um verhaltensbedingte Ergebnisse handelt.
- Zu diesem Ergebnis `Impact:S3/MaliciousIPCaller` werden API-Aufrufe vom Amazon S3 S3-Service analysiert und das `SourceIPAddress` Protokollelement mit einer Tabelle mit öffentlichen

IP-Adressen verglichen CloudTrail, die Feeds mit Bedrohungsinformationen enthält. GuardDuty Sobald es eine direkte Übereinstimmung mit einem Eintrag findet, generiert es das Ergebnis.

Wir empfehlen die Implementierung einer Mischung aus verhaltensbasierten und regelbasierten Warnmeldungen, da es nicht immer möglich ist, regelbasierte Warnmeldungen für jede Aktivität innerhalb Ihres Bedrohungsmodells zu implementieren.

Personengestützte Erkennung

Bis zu diesem Zeitpunkt haben wir über technologiegestützte Erkennung gesprochen. Die andere wichtige Erkennungsquelle sind Personen innerhalb oder außerhalb der Organisation des Kunden. Insider können als Mitarbeiter oder Auftragnehmer definiert werden, und Außenstehende sind Entitäten wie Sicherheitsforscher, Strafverfolgungsbehörden, Nachrichtendienste und soziale Medien.

Obwohl die technologiegestützte Erkennung systematisch konfiguriert werden kann, gibt es eine Vielzahl von Formen, wie z. B. E-Mails, Tickets, Post, Nachrichtenbeiträge, Telefonanrufe und persönliche Interaktionen. Es kann davon ausgegangen werden, dass technologiegestützte Erkennungsbenachrichtigungen nahezu in Echtzeit zugestellt werden, es gibt jedoch keine Zeitvorgaben für die Erkennung durch Personen. Es ist unerlässlich, dass die Sicherheitskultur personengestützte Erkennungsmechanismen einbezieht, erleichtert und unterstützt, um einen umfassenden Sicherheitsansatz zu gewährleisten.

Zusammenfassung

Bei der Erkennung ist es wichtig, eine Mischung aus regelbasierten und verhaltensorientierten Warnmeldungen zu haben. Darüber hinaus sollten Sie über Mechanismen verfügen, mit denen Personen sowohl intern als auch extern ein Ticket zu einem Sicherheitsproblem einreichen können. Menschen können eine der wertvollsten Quellen für Sicherheitsereignisse sein. Daher ist es wichtig, über Prozesse zu verfügen, mit denen Menschen Bedenken äußern können. Sie sollten die Bedrohungsmodelle Ihrer Umgebung verwenden, um mit der Erkennung von Gebäuden zu beginnen. Mithilfe von Bedrohungsmodellen können Sie Warnmeldungen erstellen, die auf Bedrohungen basieren, die für Ihre Umgebung am relevantesten sind. Schließlich können Sie Frameworks wie MITRE ATT&CK verwenden, um die Taktiken, Techniken und Verfahren von Bedrohungsakteuren zu verstehen (). TTPs Es kann hilfreich sein, das MITRE ATT&CK-Framework als gemeinsame Sprache für Ihre verschiedenen Erkennungsmechanismen zu verwenden.

Analyse

Protokolle, Abfragefunktionen und Bedrohungsinformationen sind nur einige der unterstützenden Komponenten, die für die Analysephase erforderlich sind. Viele der zur Erkennung verwendeten Protokolle werden auch für Analysen verwendet und erfordern das Onboarding und die Konfiguration von Abfragetools.

Validierung, Umfang und Bewertung der Auswirkungen der Warnung

Während der Analysephase wird eine umfassende Protokollanalyse mit dem Ziel durchgeführt, Warnmeldungen zu validieren, den Umfang zu definieren und die Auswirkungen einer möglichen Gefährdung zu bewerten.

- Die Validierung der Warnung ist der Ausgangspunkt der Analysephase. Incident-Responder werden nach Protokolleinträgen aus verschiedenen Quellen suchen und sich direkt mit den Eigentümern der betroffenen Workloads in Verbindung setzen.
- Die Festlegung des Geltungsbereichs ist der nächste Schritt, bei dem alle beteiligten Ressourcen inventarisiert und die Kritikalität der Warnmeldungen angepasst wird, nachdem sich die Beteiligten einig sind, dass es sich wahrscheinlich nicht um ein falsches Positivsignal handelt.
- Schließlich wird in der Folgenabschätzung die tatsächliche Betriebsunterbrechung detailliert beschrieben.

Sobald die betroffenen Workload-Komponenten identifiziert sind, können die Ergebnisse des Scopings mit dem Recovery Point Objective (RPO) und dem Recovery Time Objective (RTO) des jeweiligen Workloads korreliert werden. Dabei wird die Wichtigkeit der Alerts berücksichtigt, wodurch die Ressourcenzuweisung und alle weiteren Aktivitäten eingeleitet werden. Nicht alle Vorfälle beeinträchtigen unmittelbar den Betrieb eines Workloads, der einen Geschäftsprozess unterstützt. Vorfälle wie die Offenlegung vertraulicher Daten, der Diebstahl geistigen Eigentums oder die Entführung von Ressourcen (wie beim Mining von Kryptowährungen) können einen Geschäftsprozess möglicherweise nicht sofort stoppen oder schwächen, können jedoch zu einem späteren Zeitpunkt Konsequenzen haben.

Reichern Sie Sicherheitsprotokolle und Ergebnisse an

Bereicherung mit Bedrohungsinformationen und organisatorischem Kontext

Im Laufe der Analyse müssen die interessierenden Observablen angereichert werden, um die Warnung besser kontextualisieren zu können. Wie im Abschnitt Vorbereitung beschrieben, kann die

Integration und Nutzung von Informationen über Cyberbedrohungen hilfreich sein, um mehr über eine Sicherheitsfeststellung zu erfahren. Threat Intelligence Services werden verwendet, um öffentlichen IP-Adressen, Domainnamen und Datei-Hashes Reputation und Eigentumsrechte zuzuweisen. Diese Tools sind als kostenpflichtige und als kostenlose Dienste erhältlich.

Kunden, die Amazon Athena als Tool zur Protokollabfrage verwenden, profitieren von den Vorteilen von AWS Glue-Jobs, um Bedrohungsinformationen als Tabellen zu laden. Die Threat-Intelligence-Tabellen können in SQL-Abfragen verwendet werden, um Protokollelemente wie IP-Adressen und Domainnamen zu korrelieren und so eine erweiterte Ansicht der zu analysierenden Daten zu erhalten.

AWS GuardDuty stellt Kunden keine Bedrohungsinformationen direkt zur Verfügung, aber Dienste wie Amazon nutzen Bedrohungsinformationen zur Anreicherung und Generierung von Erkenntnissen. Sie können auch benutzerdefinierte Bedrohungslisten hochladen, die auf Ihren eigenen Bedrohungsinformationen GuardDuty basieren.

Bereicherung durch Automatisierung

Automatisierung ist ein integraler Bestandteil der AWS Cloud Unternehmensführung. Sie kann in den verschiedenen Phasen des Incident-Response-Lebenszyklus eingesetzt werden.

In der Erkennungsphase gleicht die regelbasierte Automatisierung anhand von Protokollen die für das Bedrohungsmodell relevanten Muster ab und ergreift geeignete Maßnahmen, z. B. das Senden von Benachrichtigungen. In der Analysephase kann der Erkennungsmechanismus genutzt und die Warnmeldung an eine Engine weitergeleitet werden, die in der Lage ist, Protokolle abzufragen und Observables zur Kontextualisierung des Ereignisses anzureichern.

Die Warnstelle besteht in ihrer grundlegenden Form aus einer Ressource und einer Identität. Beispielsweise könnten Sie eine Automatisierung implementieren, um AWS API-Aktivitäten abzufragen CloudTrail , die von der Identität oder Ressource der Warnmeldungsstelle zum Zeitpunkt der Warnung ausgeführt wurden. Dadurch erhalten Sie zusätzliche Einblicke`eventSource`, einschließlich`eventName`,`SourceIPAddress`, und `userAgent` identifizierter API-Aktivitäten. Durch die automatisierte Ausführung dieser Abfragen können Responder Zeit bei der Triage sparen und zusätzlichen Kontext erhalten, um fundiertere Entscheidungen treffen zu können.

Im Blogbeitrag Wie man AWS Security Hub Hub-Ergebnisse mit Konto-Metadaten anreichert, finden Sie ein Beispiel dafür, wie Sie mithilfe von Automatisierung Sicherheitsergebnisse anreichern und Analysen vereinfachen können.

Sammeln und analysieren Sie forensische Beweise

Forensik ist, wie im the section called “Vorbereitung” Abschnitt dieses Dokuments erwähnt, der Prozess der Erfassung und Analyse von Artefakten bei der Reaktion auf Vorfälle. On AWS ist auf Infrastrukturdomänenressourcen wie die Erfassung von Netzwerkdatenverkehrspaketen, Speicherabbilder des Betriebssystems und für Dienstdomänenressourcen wie Protokolle anwendbar. AWS CloudTrail

Der forensische Prozess weist die folgenden grundlegenden Merkmale auf:

- Konsistent — Er folgt exakt den dokumentierten Schritten, ohne Abweichungen.
- Wiederholbar — Es führt zu exakt den gleichen Ergebnissen, wenn es gegen dasselbe Artefakt wiederholt wird.
- Üblich — Es ist öffentlich dokumentiert und weit verbreitet.

Es ist wichtig, dass für Artefakte, die bei der Reaktion auf Vorfälle gesammelt wurden, eine Kontrollkette eingehalten wird. Neben der Speicherung der Artefakte in schreibgeschützten Repositorys können Automatisierung und die automatische Generierung der Dokumentation dieser Sammlung hilfreich sein. Die Analyse sollte nur an exakten Replikaten der gesammelten Artefakte durchgeführt werden, um die Integrität zu wahren.

Sammeln Sie relevante Artefakte

Unter Berücksichtigung dieser Merkmale und auf der Grundlage der entsprechenden Warnmeldungen und der Bewertung der Auswirkungen und des Umfangs müssen Sie die Daten sammeln, die für weitere Untersuchungen und Analysen relevant sind. Verschiedene Arten und Quellen von Daten, die für eine Untersuchung relevant sein könnten, darunter service/control Ebenenprotokolle (CloudTrail, Amazon S3 S3-Datenereignisse, VPC Flow Logs), Daten (Amazon S3 S3-Metadaten und Objekte) und Ressourcen (Datenbanken, Amazon EC2 EC2-Instances).

Service/control Flugzeug-Logs können für lokale Analysen gesammelt oder idealerweise direkt über native AWS Dienste (falls zutreffend) abgefragt werden. Daten (einschließlich Metadaten) können direkt abgefragt werden, um relevante Informationen zu erhalten oder die Quellobjekte abzurufen. Verwenden Sie beispielsweise die, AWS CLI um Amazon S3 S3-Bucket- und Objektmetadaten abzurufen und Quellobjekte direkt abzurufen. Ressourcen müssen auf eine Weise gesammelt werden, die dem Ressourcentyp und der beabsichtigten Analysemethode entspricht. Datenbanken können beispielsweise gesammelt werden, indem ein copy/snapshot System erstellt wird, auf dem die Datenbank ausgeführt wird, ein System mit copy/snapshot der gesamten Datenbank selbst oder

durch Abfragen und Extrahieren bestimmter Daten und Protokolle aus der Datenbank, die für die Untersuchung relevant sind.

Für Amazon EC2 EC2-Instances gibt es einen bestimmten Datensatz, der gesammelt werden sollte, und eine bestimmte Reihenfolge der Erfassung, die durchgeführt werden sollte, um die größtmögliche Menge an Daten für Analysen und Untersuchungen zu erfassen und aufzubewahren.

Konkret lautet die Reihenfolge, in der die Antwort die meisten Daten aus einer Amazon EC2 EC2-Instance abruft und speichert, wie folgt:

1. Instance-Metadaten abrufen — Erfassen Sie Instance-Metadaten, die für die Untersuchung und Datenabfragen relevant sind (Instance-ID, Typ, IP-Adresse, VPC/subnet ID, Region, Amazon Machine Image (AMI) -ID, angehängte Sicherheitsgruppen, Startzeit).
2. Instanzschutz und Tags aktivieren — Aktivieren Sie Instance-Schutzmaßnahmen wie Kündigungsschutz, Einstellung des Shutdown-Verhaltens auf Stopp (falls auf Beenden gesetzt), Deaktivieren von Delete on Termination-Attributen für die angehängten EBS-Volumes und Anwenden geeigneter Tags sowohl für die visuelle Kennzeichnung als auch für die Verwendung in möglichen Reaktionsautomatisierungen (z. B. beim Anwenden eines Tags mit dem Namen `Status` und Wert von`Quarantine`, führen Sie eine forensische Erfassung von Daten durch und isolieren Sie die Instanz).
3. Festplatte abrufen (EBS-Snapshots) — Erfassen Sie einen EBS-Snapshot der angehängten EBS-Volumes. Jeder Snapshot enthält die Informationen, die Sie benötigen, um Ihre Daten (ab dem Zeitpunkt, an dem der Snapshot erstellt wurde) auf einem neuen EBS-Volume wiederherzustellen. Sehen Sie sich den Schritt zur Durchführung der response/artifact Live-Erfassung an, wenn Sie Instance-Speicher-Volumes verwenden.
4. Speicher abrufen — Da EBS-Snapshots nur Daten erfassen, die auf Ihr Amazon EBS-Volume geschrieben wurden, was möglicherweise Daten ausschließt, die von Ihren Anwendungen oder Ihrem Betriebssystem im Speicher gespeichert oder zwischengespeichert werden, ist es unerlässlich, ein Systemspeicher-Image mit einem geeigneten Open-Source-oder kommerziellen Tool eines Drittanbieters zu erwerben, um verfügbare Daten aus dem System abzurufen.
5. (Optional) Live-Antwort-/Artefakterfassung durchführen — Führen Sie eine gezielte Datenerfassung (disk/memory/logs) über Live-Response auf dem System nur durch, wenn Festplatte oder Arbeitsspeicher nicht anderweitig abgerufen werden können oder wenn ein triftiger geschäftlicher oder betrieblicher Grund vorliegt. Dadurch werden wertvolle Systemdaten und Artefakte verändert.

6. Instance außer Betrieb nehmen — Trennen Sie die Instance von Auto Scaling Scaling-Gruppen, heben Sie die Registrierung der Instance bei Load Balancers auf und passen Sie ein vorgefertigtes Instance-Profil mit minimierten oder keinen Berechtigungen an oder wenden Sie es an.
7. Instanz isolieren oder eindämmen — Stellen Sie sicher, dass die Instanz effektiv von anderen Systemen und Ressourcen in der Umgebung isoliert ist, indem Sie aktuelle und future Verbindungen zu und von der Instance beenden und verhindern. Weitere Informationen finden Sie the section called “Eindämmung” im Abschnitt dieses Dokuments.
8. Wahl des Responders — Wählen Sie je nach Situation und Zielen eine der folgenden Optionen aus:
   - Das System außer Betrieb nehmen und herunterfahren (empfohlen).

     Schalten Sie das System ab, sobald die verfügbaren Beweise vorliegen, um zu überprüfen, wie die Instanz am wirksamsten gegen mögliche future Auswirkungen auf die Umwelt vorbeugen kann.
   - Führen Sie die Instance weiterhin in einer isolierten Umgebung aus, die für die Überwachung instrumentiert ist.

     Es wird zwar nicht als Standardansatz empfohlen, aber wenn eine Situation eine kontinuierliche Beobachtung der Instance erfordert (z. B. wenn zusätzliche Daten oder Indikatoren für eine umfassende Untersuchung und Analyse der Instance benötigt werden), können Sie erwägen, die Instance herunterzufahren, ein AMI der Instance zu erstellen und die Instance in Ihrem speziellen forensischen Konto in einer Sandbox-Umgebung neu zu starten, die so konfiguriert ist, dass sie vollständig isoliert und mit Instrumentierung konfiguriert ist, um eine nahezu kontinuierliche Überwachung der Instance zu ermöglichen. (für Beispiel: VPC Flow Logs oder VPC Traffic Mirroring).

> **Note**
>
> Um verfügbare flüchtige (und wertvolle) Daten zu erfassen, ist es wichtig, den Arbeitsspeicher vor Live-Reaktionsaktivitäten oder der Systemisolierung oder dem Herunterfahren zu erfassen.

Entwickeln Sie Erzählungen

Dokumentieren Sie während der Analyse und Untersuchung die ergriffenen Maßnahmen, die durchgeführten Analysen und die identifizierten Informationen, die in den nachfolgenden Phasen

und schließlich in einem Abschlussbericht verwendet werden können. Diese Schilderungen sollten kurz und präzise sein und bestätigen, dass relevante Informationen enthalten sind, um ein effektives Verständnis des Vorfalls zu gewährleisten und einen genauen Zeitplan einzuhalten. Sie sind auch hilfreich, wenn Sie Personen außerhalb des Kernteams für die Reaktion auf Vorfälle einbeziehen. Ein Beispiel:

> Die Marketing- und Vertriebsabteilung erhielt am 15. März 2022 eine Lösegeldforderung, in der die Zahlung in Kryptowährung gefordert wurde, um die öffentliche Veröffentlichung möglicher sensibler Daten zu verhindern. Das SOC stellte fest, dass die Amazon RDS-Datenbank, die zu Marketing und Vertrieb gehört, am 20. Februar 2022 öffentlich zugänglich war. Das SOC fragte die RDS-Zugriffsprotokolle ab und stellte fest, dass die IP-Adresse 198.51.100.23 am 20. Februar 2022 mit den Anmeldeinformationen von Major Mary, einer der Webentwicklerinnen*mm03434*, verwendet wurde. Das SOC hat VPC Flow Logs abgefragt und festgestellt, dass ungefähr 256 MB an Daten am selben Tag an dieselbe IP-Adresse übertragen wurden (Zeitstempel 20.02.20T 15:50 +00Z). Das SOC hat anhand von Open-Source-Bedrohungsinformationen festgestellt, dass die Anmeldeinformationen derzeit im Klartext im öffentlichen Repository verfügbar sind. *https[:]//example[.]com/majormary/rds-utils*

Eindämmung

Eine Definition von Eindämmung in Bezug auf die Reaktion auf Vorfälle ist der Prozess oder die Implementierung einer Strategie bei der Behandlung eines Sicherheitsereignisses, die darauf abzielt, den Umfang des Sicherheitsereignisses zu minimieren und die Auswirkungen einer unbefugten Nutzung innerhalb der Umgebung einzudämmen.

Eine Eindämmungsstrategie hängt von einer Vielzahl von Faktoren ab und kann sich von Organisation zu Organisation in Bezug auf die Anwendung der Eindämmungstaktiken, den Zeitpunkt und den Zweck unterscheiden. Der NIST SP 800-61 Leitfaden zur Behandlung von Computersicherheitsvorfällen beschreibt mehrere Kriterien für die Bestimmung der geeigneten Eindämmungsstrategie, darunter:

- Mögliche Beschädigung und Diebstahl von Ressourcen
- Notwendigkeit der Beweissicherung
- Verfügbarkeit von Diensten (Netzwerkkonnektivität, für externe Parteien bereitgestellte Dienste)
- Zeit und Ressourcen, die für die Umsetzung der Strategie benötigt wurden

- Wirksamkeit der Strategie (teilweise oder vollständige Eindämmung)
- Dauer der Lösung (Notfalllösung muss innerhalb von vier Stunden entfernt werden, vorübergehende Behelfslösung muss in zwei Wochen entfernt werden, permanente Lösung)

Hinsichtlich der verfügbaren AWS Dienste lassen sich die grundlegenden Maßnahmen zur Eindämmung jedoch in drei Kategorien unterteilen:

- Eingrenzung von Quellen — Verwenden Sie Filter und Routing, um den Zugriff von einer bestimmten Quelle aus zu verhindern.
- Technik und Zugriffskontrolle — Sperren Sie den Zugriff, um unbefugten Zugriff auf die betroffenen Ressourcen zu verhindern.
- Zieleindämmung — Verwenden Sie Filterung und Routing, um den Zugriff auf eine Zielressource zu verhindern.

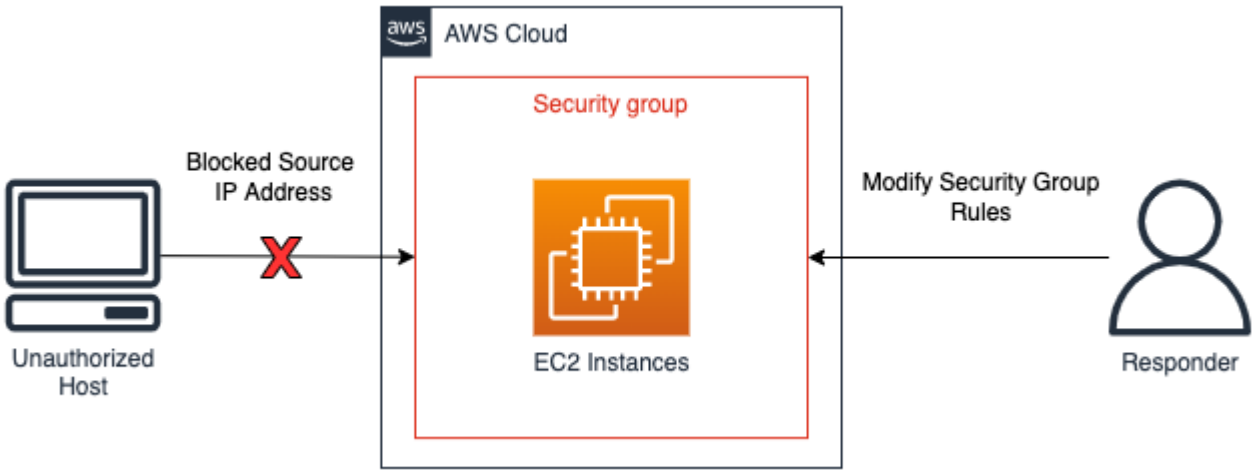
Quell-Containment

Quelleneinhausung ist die Verwendung und Anwendung von Filtern oder Routing innerhalb einer Umgebung, um den Zugriff auf Ressourcen von einer bestimmten Quell-IP-Adresse oder einem bestimmten Netzwerkbereich aus zu verhindern. Beispiele für die Eingrenzung von Quellen mithilfe von AWS Diensten werden hier hervorgehoben:

- Sicherheitsgruppen — Das Erstellen und Anwenden isolierter Sicherheitsgruppen auf Amazon EC2 EC2-Instances oder das Entfernen von Regeln aus einer vorhandenen Sicherheitsgruppe kann dazu beitragen, unbefugten Datenverkehr zu einer Amazon EC2 EC2-Instance oder AWS -Ressource einzudämmen. Es ist wichtig zu beachten, dass bestehende nachverfolgte Verbindungen nicht aufgrund wechselnder Sicherheitsgruppen geschlossen werden — nur future Datenverkehr wird von der neuen Sicherheitsgruppe effektiv blockiert (weitere Informationen zu verfolgten und nicht verfolgten Verbindungen finden Sie in diesem Incident Response Playbook und in der Verbindungsverfolgung von Sicherheitsgruppen).
- Richtlinien — Amazon S3 S3-Bucket-Richtlinien können so konfiguriert werden, dass sie Datenverkehr von einer IP-Adresse, einem Netzwerkbereich oder einem VPC-Endpunkt blockieren oder zulassen. Richtlinien ermöglichen es, verdächtige Adressen und den Zugriff auf den Amazon S3 S3-Bucket zu blockieren. Weitere Informationen zu Bucket-Richtlinien finden Sie unter Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole.
- AWS WAF — Web-Zugriffskontrolllisten (Web ACLs) können konfiguriert werden AWS WAF , um eine detaillierte Kontrolle über Webanfragen zu ermöglichen, auf die Ressourcen antworten.

Sie können einem IP-Set, für das konfiguriert ist AWS WAF, eine IP-Adresse oder einen Netzwerkbereich hinzufügen und Vergleichsbedingungen wie Sperren auf den IP-Satz anwenden. Dadurch werden Webanfragen an eine Ressource blockiert, wenn die IP-Adresse oder die Netzwerkbereiche des ursprünglichen Datenverkehrs mit den in den IP-Set-Regeln konfigurierten Bereichen übereinstimmen.

Ein Beispiel für die Eindämmung von Quellen ist in der folgenden Abbildung zu sehen. Ein Incident-Response-Analyst ändert eine Sicherheitsgruppe einer Amazon EC2 EC2-Instance, um neue Verbindungen nur auf bestimmte IP-Adressen zu beschränken. Wie im Aufzähler Sicherheitsgruppen angegeben, werden bestehende nachverfolgte Verbindungen nicht aufgrund von Änderungen der Sicherheitsgruppen heruntergefahren.



Beispiel für eine Quellensperre

> **Note**
>
> Sicherheitsgruppen und Netzwerk-ACLs filtern keinen Datenverkehr zu Amazon Route 53 Wenn Sie eine EC2-Instance enthalten und verhindern möchten, dass diese externe Hosts kontaktiert, stellen Sie sicher, dass Sie auch die DNS-Kommunikation explizit blockieren.

Technik und Eingrenzung des Zugriffs

Verhindern Sie die unbefugte Nutzung einer Ressource, indem Sie die Funktionen und IAM-Prinzipale einschränken, die Zugriff auf die Ressource haben. Dazu gehört die Einschränkung der Berechtigungen von IAM-Prinzipalen, die Zugriff auf die Ressource haben. Dazu gehört auch

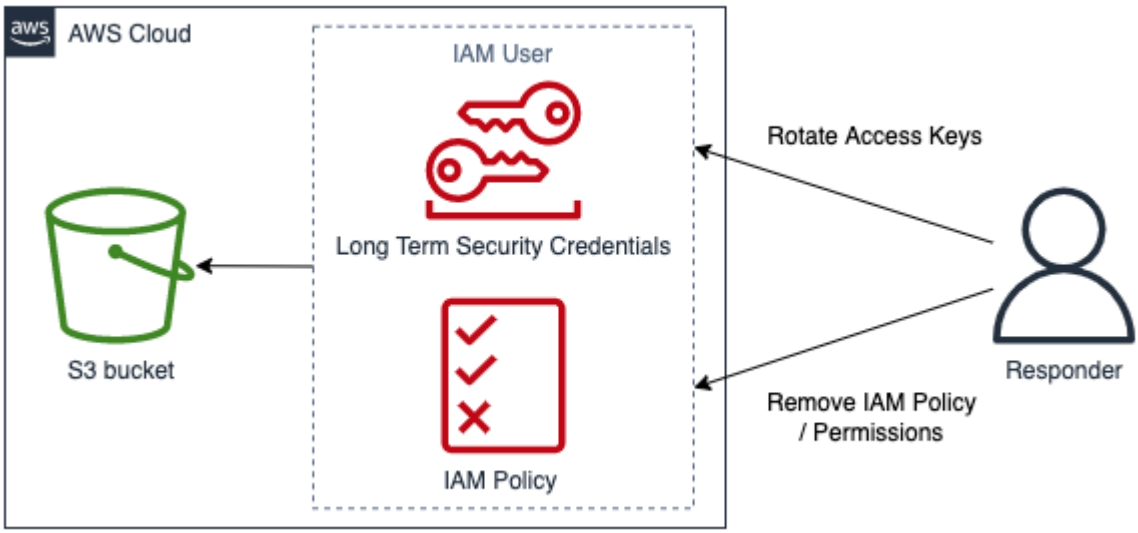
der vorübergehende Widerruf von Sicherheitsanmeldeinformationen. Beispiele für Technik und Zugriffskontrolle mithilfe von AWS Diensten werden hier hervorgehoben:

- Berechtigungen einschränken — Die einem IAM-Prinzipal zugewiesenen Berechtigungen sollten dem Prinzip der geringsten Rechte entsprechen. Während eines aktiven Sicherheitsereignisses müssen Sie jedoch möglicherweise den Zugriff auf eine Zielressource von einem bestimmten IAM-Prinzipal aus noch weiter einschränken. In diesem Fall ist es möglich, den Zugriff auf eine Ressource einzuschränken, indem dem IAM-Prinzipal die entsprechenden Berechtigungen entzogen werden. Dies erfolgt mit dem IAM-Dienst und kann mithilfe des AWS-Managementkonsole AWS CLI, des oder eines AWS SDK angewendet werden.
- Schlüssel widerrufen — IAM-Zugriffsschlüssel werden von IAM-Prinzipalen für den Zugriff auf oder die Verwaltung von Ressourcen verwendet. Dabei handelt es sich um langfristige statische Anmeldeinformationen zum Signieren programmatischer Anfragen an die AWS CLIAWS OR-API. Sie beginnen mit dem Präfix AKIA (weitere Informationen finden Sie im Abschnitt Grundlegendes zu eindeutigen ID-Präfixen unter IAM-Identifikatoren). Um den Zugriff für einen IAM-Prinzipal einzuschränken, wenn ein IAM-Zugriffsschlüssel kompromittiert wurde, kann der Zugriffsschlüssel deaktiviert oder gelöscht werden. Es ist wichtig, Folgendes zu beachten:
  - Ein Zugriffsschlüssel kann reaktiviert werden, nachdem er deaktiviert wurde.
  - Ein Zugriffsschlüssel kann nicht wiederhergestellt werden, sobald er gelöscht wurde.
  - Ein IAM-Prinzipal kann bis zu zwei Zugriffsschlüssel gleichzeitig haben.
  - Benutzer oder Anwendungen, die den Zugriffsschlüssel verwenden, verlieren den Zugriff, sobald der Schlüssel entweder deaktiviert oder gelöscht wird.
- Temporäre Sicherheitsanmeldedaten widerrufen — Temporäre Sicherheitsanmeldedaten können von einer Organisation verwendet werden, um den Zugriff auf AWS Ressourcen zu kontrollieren. Sie beginnen mit dem Präfix ASIA (weitere Informationen finden Sie im Abschnitt Grundlegendes zu eindeutigen ID-Präfixen unter IAM-Identifikatoren). Temporäre Anmeldeinformationen werden in der Regel von IAM-Rollen verwendet und müssen nicht rotiert oder explizit gesperrt werden, da sie eine begrenzte Lebensdauer haben. In Fällen, in denen vor Ablauf der temporären Anmeldeinformationen ein Sicherheitsereignis eintritt, müssen Sie möglicherweise die effektiven Berechtigungen der vorhandenen temporären Anmeldeinformationen ändern. Dies kann mithilfe des darin enthaltenen IAM-Dienstes abgeschlossen werden. AWS-Managementkonsole Temporäre Sicherheitsanmeldedaten können auch für IAM-Benutzer ausgestellt werden (im Gegensatz zu IAM-Rollen). Zum Zeitpunkt der Erstellung dieses Artikels gibt es jedoch keine Möglichkeit, die temporären Sicherheitsanmeldedaten für einen IAM-Benutzer innerhalb von zu widerrufen. AWS-Managementkonsole Bei Sicherheitsereignissen, bei denen der IAM-Zugriffsschlüssel eines Benutzers durch einen nicht autorisierten Benutzer kompromittiert wird, der temporäre

Sicherheitsanmeldedaten erstellt hat, können die temporären Sicherheitsanmeldedaten auf zwei Arten gesperrt werden:

  - Fügen Sie dem IAM-Benutzer eine Inline-Richtlinie hinzu, die den Zugriff auf die Dauer der Ausgabe des Sicherheitstokens verhindert (weitere Informationen finden Sie im Abschnitt Sperren des Zugriffs auf temporäre Sicherheitsanmeldeinformationen, die vor einem bestimmten Zeitpunkt ausgestellt wurden, unter Berechtigungen für temporäre Sicherheitsanmeldeinformationen deaktivieren).
  - Löschen Sie den IAM-Benutzer, dem die kompromittierten Zugriffsschlüssel gehören. Erstellen Sie den Benutzer bei Bedarf erneut.
- AWS WAF- Bestimmte Techniken, die von nicht autorisierten Benutzern eingesetzt werden, beinhalten häufig auftretende bösartige Datenverkehrsmuster, wie z. B. Anfragen, die SQL-Injection und Cross-Site Scripting (XSS) beinhalten. AWS WAF kann mithilfe der integrierten Regelanweisungen so konfiguriert werden, dass der Datenverkehr mithilfe dieser Techniken abgeglichen und abgewiesen wird AWS WAF .

Ein Beispiel für Technik und Zugriffskontrolle finden Sie in der folgenden Abbildung. Ein Incident-Responder rotiert die Zugriffsschlüssel oder entfernt eine IAM-Richtlinie, um zu verhindern, dass ein IAM-Benutzer auf einen Amazon S3 S3-Bucket zugreift.



Beispiel für Technik und Zugangskontrolle

Eindämmung des Ziels

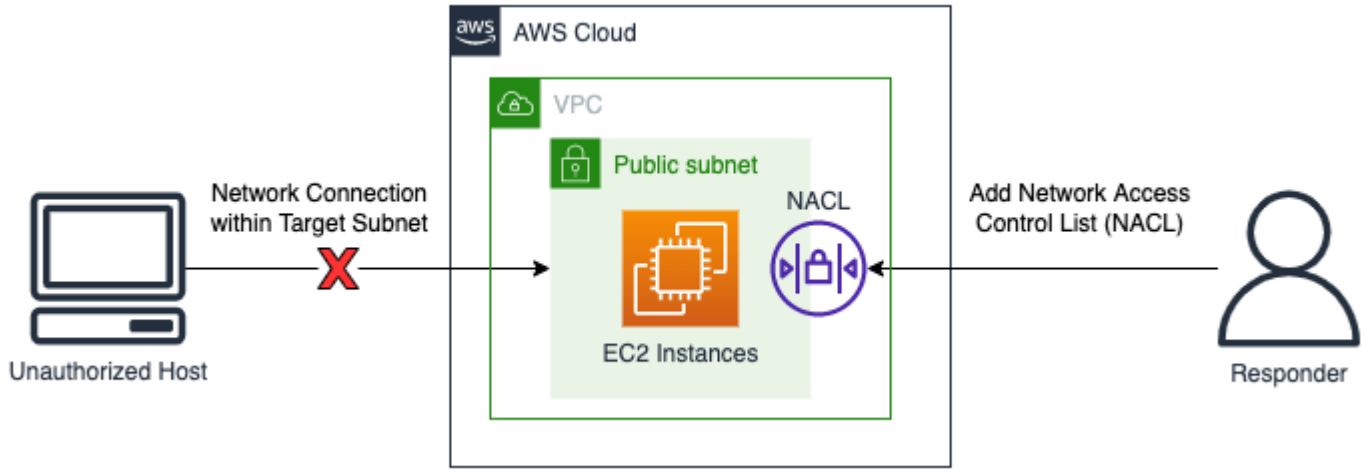
Unter Destination Containment versteht man die Anwendung von Filterung oder Routing innerhalb einer Umgebung, um den Zugriff auf einen Zielhost oder eine Zielressource zu verhindern. In einigen

Fällen beinhaltet die Eindämmung von Zielen auch eine Form der Resilienz, um zu überprüfen, ob legitime Ressourcen repliziert werden, um ihre Verfügbarkeit sicherzustellen. Ressourcen sollten aus Gründen der Isolierung und Eindämmung von diesen Formen der Resilienz getrennt werden. Zu den Beispielen für die Eindämmung von Zielen mithilfe von Diensten gehören: AWS

- Netzwerk ACLs — Für Netzwerke ACLs (Netzwerke ACLs), die in Subnetzen konfiguriert sind, die AWS Ressourcen enthalten, können Ablehnungsregeln hinzugefügt werden. Diese Ablehnungsregeln können angewendet werden, um den Zugriff auf eine bestimmte AWS Ressource zu verhindern. Die Anwendung der Network Access Control List (Network ACL) wirkt sich jedoch auf alle Ressourcen im Subnetz aus, nicht nur auf die Ressourcen, auf die ohne Autorisierung zugegriffen wird. Regeln, die in einer Netzwerk-ACL aufgeführt sind, werden von oben nach unten verarbeitet. Daher sollte die erste Regel in einer vorhandenen Netzwerk-ACL so konfiguriert werden, dass nicht autorisierter Datenverkehr zur Zielressource und zum Zielsubnetz verweigert wird. Alternativ kann eine völlig neue Netzwerk-ACL mit einer einzigen Ablehnungsregel für eingehenden und ausgehenden Verkehr erstellt und dem Subnetz zugeordnet werden, das die Zielressource enthält, um den Zugriff auf das Subnetz mithilfe der neuen Netzwerk-ACL zu verhindern.
- Herunterfahren — Das vollständige Herunterfahren einer Ressource kann wirksam sein, um die Auswirkungen einer unbefugten Nutzung einzudämmen. Das Herunterfahren einer Ressource verhindert auch den legitimen Zugriff für geschäftliche Zwecke und verhindert, dass flüchtige forensische Daten abgerufen werden. Daher sollte dies eine gezielte Entscheidung sein und anhand der Sicherheitsrichtlinien eines Unternehmens beurteilt werden.
- Isolierung VPCs — Isolierte VPCs können verwendet werden, um Ressourcen effektiv einzudämmen und gleichzeitig Zugriff auf legitimen Datenverkehr zu gewähren (z. B. Antiviren- (AV) - oder EDR-Lösungen, die Zugriff auf das Internet oder eine externe Managementkonsole erfordern). Isolierte VPCs können vor einem Sicherheitsereignis so vorkonfiguriert werden, dass gültige IP-Adressen und Ports zugelassen werden, und gezielte Ressourcen können während eines aktiven Sicherheitsereignisses sofort in diese Isolierungs-VPC verschoben werden, um die Ressource einzudämmen und gleichzeitig zu ermöglichen, dass legitimer Datenverkehr von der Zielressource in nachfolgenden Phasen der Reaktion auf Vorfälle gesendet und empfangen werden kann. Ein wichtiger Aspekt bei der Verwendung einer isolierten VPC besteht darin, dass Ressourcen wie EC2-Instances vor der Verwendung in der neuen isolierten VPC heruntergefahren und neu gestartet werden müssen. Bestehende EC2-Instances können nicht in eine andere VPC oder eine andere Availability Zone verschoben werden. Folgen Sie dazu den unter Wie verschiebe ich meine Amazon EC2 EC2-Instance in ein anderes Subnetz, eine Availability Zone oder eine VPC? beschriebenen Schritte.

- Auto Scaling Scaling-Gruppen und Load Balancer — AWS Ressourcen, die Auto Scaling Scaling-Gruppen und Load Balancern zugeordnet sind, sollten im Rahmen der Zielbeschränkungen getrennt und deregistriert werden. Das Trennen und Deregistrieren von AWS Ressourcen kann mit dem SDK, und durchgeführt werden. AWS-Managementkonsole AWS CLI AWS

Das folgende Diagramm zeigt ein Beispiel für die Eindämmung von Zielen. Ein Incident Response Analyst fügt einem Subnetz eine Netzwerk-ACL hinzu, um eine Netzwerkverbindungsanfrage von einem nicht autorisierten Host zu blockieren.



Beispiel für die Eindämmung eines Ziels

Zusammenfassung

Die Eindämmung ist ein Schritt der Reaktion auf Vorfälle und kann manuell oder automatisiert erfolgen. Die allgemeine Eindämmungsstrategie sollte sich an den Sicherheitsrichtlinien und Geschäftsanforderungen eines Unternehmens orientieren und sicherstellen, dass negative Auswirkungen vor der Beseitigung und Wiederherstellung so effizient wie möglich abgemildert werden.

Beseitigung

Bei der Beseitigung von Sicherheitsvorfällen handelt es sich um die Entfernung verdächtiger oder nicht autorisierter Ressourcen, um das Konto wieder in einen bekannten sicheren Zustand zu versetzen. Die Strategie zur Beseitigung hängt von mehreren Faktoren ab, die von den Geschäftsanforderungen Ihres Unternehmens abhängen.

Der NIST SP 800-61 Leitfaden zur Behandlung von Computersicherheitsvorfällen enthält mehrere Schritte zur Beseitigung:

1. Identifizieren und beheben Sie alle Sicherheitslücken, die ausgenutzt wurden.
2. Entfernen Sie Malware, unangemessene Materialien und andere Komponenten.
3. Wenn weitere betroffene Hosts entdeckt werden (z. B. neue Malware-Infektionen), wiederholen Sie die Erkennungs- und Analyseschritte, um alle anderen betroffenen Hosts zu identifizieren und den Vorfall dann einzudämmen und zu beseitigen.

Bei AWS Ressourcen kann dies anhand der Ereignisse, die mithilfe verfügbarer Protokolle oder automatisierter Tools wie CloudWatch Logs und Amazon GuardDuty erkannt und analysiert werden, weiter verfeinert werden. Diese Ereignisse sollten als Grundlage für die Entscheidung dienen, welche Abhilfemaßnahmen durchgeführt werden sollten, um die Umgebung ordnungsgemäß wieder in einen bekannten sicheren Zustand zu versetzen.

Im ersten Schritt der Ausrottung wird festgestellt, welche Ressourcen innerhalb des AWS Kontos betroffen sind. Dies wird durch die Analyse Ihrer verfügbaren Protokolldatenquellen und Ressourcen und automatisierter Tools erreicht.

- Identifizieren Sie nicht autorisierte Aktionen, die von den IAM-Identitäten in Ihrem Konto ausgeführt wurden.
- Identifizieren Sie unbefugte Zugriffe oder Änderungen an Ihrem Konto.
- Identifizieren Sie die Erstellung nicht autorisierter Ressourcen oder IAM-Benutzer.
- Identifizieren Sie Systeme oder Ressourcen mit nicht autorisierten Änderungen.

Sobald die Liste der Ressourcen identifiziert ist, sollten Sie jede einzelne überprüfen, um festzustellen, welche Auswirkungen das Löschen oder Wiederherstellen der Ressource auf Ihr Unternehmen hat. Wenn beispielsweise ein Webserver Ihre Geschäftsanwendung hostet und das Löschen dieser Anwendung zu Ausfallzeiten führen würde, sollten Sie erwägen, die Ressource aus verifizierten sicheren Backups wiederherzustellen oder das System von einem sauberen AMI aus neu zu starten, bevor Sie den betroffenen Server löschen.

Sobald Sie Ihre Geschäftsauswirkungsanalyse abgeschlossen haben, sollten Sie anhand der Ereignisse aus Ihrer Protokollanalyse die Konten überprüfen und die entsprechenden Abhilfemaßnahmen durchführen, z. B.:

- Schlüssel rotieren oder löschen — durch diesen Schritt wird dem Akteur die Möglichkeit genommen, weiterhin Aktivitäten innerhalb des Accounts auszuführen.
- Potenziell nicht autorisierte IAM-Benutzeranmeldedaten rotieren.

- Löschen Sie unbekannte oder nicht autorisierte Ressourcen.

> **Important**
>
> Wenn Sie Ressourcen für Ihre Untersuchung behalten müssen, sollten Sie erwägen, diese Ressourcen zu sichern. Wenn Sie beispielsweise aus regulatorischen, behördlichen oder rechtlichen Gründen eine Amazon EC2 EC2-Instance behalten müssen, erstellen Sie einen Amazon EBS-Snapshot, bevor Sie die Instance entfernen.

- Bei Malware-Infektionen müssen Sie sich möglicherweise an einen AWS Partner oder einen anderen Anbieter wenden. AWS bietet keine systemeigenen Tools zur Analyse oder Entfernung von Malware. Wenn Sie jedoch das GuardDuty Malware-Modul für Amazon EBS verwenden, sind möglicherweise Empfehlungen für die bereitgestellten Ergebnisse verfügbar.

Sobald Sie die identifizierten betroffenen Ressourcen gelöscht haben, AWS empfiehlt Ihnen, eine Sicherheitsüberprüfung Ihres Kontos durchzuführen. Dies kann mithilfe von AWS Config Regeln, mithilfe von Open-Source-Lösungen wie Prowler und/oder durch andere Anbieter ScoutSuite geschehen. Sie sollten auch in Betracht ziehen, Sicherheitslücken in Ihren öffentlich zugänglichen Ressourcen (Internet) zu scannen, um das Restrisiko einzuschätzen.

Die Beseitigung ist ein Schritt der Reaktion auf Vorfälle und kann je nach Vorfall und betroffenen Ressourcen manuell oder automatisiert erfolgen. Die Gesamtstrategie sollte sich an den Sicherheitsrichtlinien und Geschäftsanforderungen eines Unternehmens orientieren und sicherstellen, dass negative Auswirkungen durch das Entfernen ungeeigneter Ressourcen oder Konfigurationen gemildert werden.

Wiederherstellung

Bei der Wiederherstellung werden Systeme in einen bekannten sicheren Zustand zurückversetzt, wobei vor der Wiederherstellung überprüft wird, ob Backups sicher sind oder nicht vom Vorfall betroffen sind. Außerdem werden Tests durchgeführt, um sicherzustellen, dass die Systeme nach der Wiederherstellung ordnungsgemäß funktionieren, und die Behebung von Sicherheitslücken im Zusammenhang mit dem Sicherheitsereignis.

Die Reihenfolge der Wiederherstellung hängt von den Anforderungen Ihres Unternehmens ab. Im Rahmen des Wiederherstellungsprozesses sollten Sie eine Analyse der Geschäftsauswirkungen durchführen, um mindestens Folgendes zu ermitteln:

- Geschäftsprioritäten oder Abhängigkeiten

- Der Sanierungsplan
- Authentifizierung und Autorisierung

Der NIST SP 800-61 Leitfaden zur Behandlung von Computersicherheitsvorfällen enthält mehrere Schritte zur Wiederherstellung von Systemen, darunter:

- Wiederherstellung von Systemen aus sauberen Backups.
  - Stellen Sie sicher, dass die Backups vor der Wiederherstellung auf den Systemen geprüft wurden, um sicherzustellen, dass die Infektion nicht vorhanden ist, und um ein erneutes Auftreten des Sicherheitsereignisses zu verhindern.

    Backups sollten im Rahmen von Disaster-Recovery-Tests regelmäßig überprüft werden, um sicherzustellen, dass der Backup-Mechanismus ordnungsgemäß funktioniert und die Datenintegrität den Wiederherstellungszielen entspricht.
  - Verwenden Sie nach Möglichkeit Backups, die vor dem Zeitstempel des ersten Ereignisses erstellt wurden, das im Rahmen der Ursachenanalyse ermittelt wurde.
- Neuaufbau von Systemen von Grund auf, einschließlich der Neubereitstellung aus einer vertrauenswürdigen Quelle mithilfe von Automatisierung, manchmal in einem neuen Konto. AWS
- Kompromittierte Dateien durch saubere Versionen ersetzen.

  Sie sollten dabei große Vorsicht walten lassen. Sie müssen absolut sicher sein, dass die Datei, die Sie wiederherstellen, als sicher gilt und von dem Vorfall nicht betroffen ist
- Patches installieren.
- Passwörter ändern.
  - Dazu gehören Passwörter für IAM-Prinzipale, die möglicherweise missbraucht wurden.
  - Wenn möglich, empfehlen wir die Verwendung von Rollen für IAM-Prinzipale und den Verbund als Teil einer Strategie der geringsten Rechte.
- Verschärfung der Netzwerkperimetersicherheit (Firewall-Regelsätze, Zugriffskontrolllisten für Boundary-Router).

Sobald die Ressourcen wiederhergestellt sind, ist es wichtig, die gewonnenen Erkenntnisse zu nutzen, um Richtlinien, Verfahren und Leitfäden zur Reaktion auf Vorfälle zu aktualisieren.

Zusammenfassend lässt sich sagen, dass es unerlässlich ist, einen Wiederherstellungsprozess zu implementieren, der die Rückkehr zu bekanntermaßen sicheren Betriebsabläufen erleichtert. Die Wiederherstellung kann lange dauern und erfordert eine enge Verknüpfung mit

Eindämmungsstrategien, um die geschäftlichen Auswirkungen gegen das Risiko einer erneuten Infektion abzuwägen. Die Wiederherstellungsverfahren sollten Schritte zur Wiederherstellung von Ressourcen und Diensten, IAM-Prinzipalen und zur Durchführung einer Sicherheitsüberprüfung des Kontos zur Bewertung des Restrisikos umfassen.

Schlussfolgerung

Jede Betriebsphase hat eigene Ziele, Techniken, Methoden und Strategien. Tabelle 4 fasst diese Phasen und einige der in diesem Abschnitt behandelten Techniken und Methoden zusammen.

Tabelle 4 — Betriebsphasen: Ziele, Techniken und Methoden

Phase	Ziel	Techniken und Methoden
Erkennung	Identifizieren eines potenziellen Sicherheitsereignisses.	• Sicherheitskontrollen zur Erkennung • Verhaltens- und regelbasierte Erkennung • Personengestützte Erkennung
Analyse	Stellen Sie fest, ob es sich bei dem Sicherheitsereignis um einen Vorfall handelt, und beurteilen Sie den Umfang des Vorfalls.	• Validierung und Umfang der Warnung • -Protokolle abfragen • Bedrohungsinformationen • Automatisierung
Eindämmung	Minimiert und begrenzt die Auswirkungen des Sicherheitsereignisses.	• Eingrenzung der Quelle • Technik und Eindämmung des Zugangs • Eindämmung des Ziels
Ausrottung	Entfernen nicht autorisierter Ressourcen oder Artefakte im Zusammenhang mit dem Sicherheitsereignis.	• Kompromittierte oder unbefugte Rotation oder Löschung von Zugangsdaten

Phase	Ziel	Techniken und Methoden
		• Unbefugtes Löschen von Ressourcen • Entfernung von Schadsoft ware • Sicherheitsscans
Wiederherstellung	Stellen Sie den zweifelsfrei funktionierenden Zustand der Systeme wieder her und überwachen Sie diese Systeme, um sicherzustellen, dass die Bedrohung nicht erneut auftritt.	• Systemwiederherstellung anhand von Backups • Systeme wurden von Grund auf neu aufgebaut • Kompromittierte Dateien wurden durch saubere Versionen ersetzt

Aktivität nach Vorfällen

Die Bedrohungslage ändert sich ständig, und es ist wichtig, dass Ihre Organisation ebenso dynamisch in der Lage ist, Ihre Umgebungen wirksam zu schützen. Der Schlüssel zur kontinuierlichen Verbesserung liegt darin, die Ergebnisse Ihrer Vorfälle und Simulationen immer wieder zu überprüfen, um Ihre Fähigkeiten zur effektiven Erkennung, Reaktion und Untersuchung möglicher Sicherheitsvorfälle zu verbessern und so Ihre möglichen Sicherheitslücken zu reduzieren, die Reaktionszeit zu verkürzen und den sicheren Betrieb wieder aufzunehmen. Mithilfe der folgenden Mechanismen können Sie überprüfen, ob Ihre Organisation über die neuesten Funktionen und Kenntnisse verfügt, um unabhängig von der Situation effektiv reagieren zu können.

Schaffen Sie einen Rahmen, um aus Vorfällen zu lernen

Die Implementierung eines Rahmens und einer Methodik aus den gewonnenen Erkenntnissen wird nicht nur dazu beitragen, die Reaktionsfähigkeit zu verbessern, sondern auch dazu beitragen, zu verhindern, dass sich der Vorfall wiederholt. Indem Sie aus jedem Vorfall lernen, können Sie verhindern, dass sich dieselben Fehler, Risiken oder Fehlkonfigurationen wiederholen. Dies verbessert nicht nur Ihre Sicherheitslage, sondern minimiert auch den Zeitverlust durch vermeidbare Situationen.

Es ist wichtig, ein Erkenntnis-Framework zu implementieren, das ganz allgemein Folgendes ermittelt und erreicht:

- Wann kommt es zu Erkenntnissen?
- Was beinhaltet der Erkenntnisprozess?
- Wie werden Erkenntnisse gewonnen?
- Wer ist auf welche Weise an dem Prozess beteiligt?
- Wie werden verbesserungswürdige Bereiche identifiziert?
- Wie stellen Sie sicher, dass die Verbesserungen effektiv verfolgt und umgesetzt werden?

Abgesehen von den aufgeführten Ergebnissen auf hoher Ebene ist es wichtig, sicherzustellen, dass Sie die richtigen Fragen stellen, um den größtmöglichen Nutzen aus dem Prozess zu ziehen (Informationen, die zu umsetzbaren Verbesserungen führen). Berücksichtigen Sie die folgenden Fragen, um Ihre Diskussionen über Erkenntnisse zu fördern:

- Was ist vorgefallen?
- Wann wurde der Vorfall zum ersten Mal identifiziert?
- Wie wurde er identifiziert?
- Von welchen Systemen wurde eine Warnung im Zusammenhang mit der Aktivität ausgegeben?
- Welche Systeme, Services und Daten waren beteiligt?
- Was ist konkret passiert?
- Was hat gut funktioniert?
- Was hat nicht gut funktioniert?
- Welcher Prozess oder welche Verfahren haben versagt oder konnten nicht skaliert werden, um auf den Vorfall zu reagieren?
- Was kann in den folgenden Bereichen verbessert werden:
  - Personen
    - Waren die Mitarbeiter, die kontaktiert werden mussten, tatsächlich verfügbar und war die Kontaktliste auf dem neuesten Stand?
    - Fehlten den Mitarbeitern Schulungen oder Fähigkeiten, die erforderlich waren, um effektiv auf den Vorfall reagieren und ihn untersuchen zu können?
    - Waren die erforderlichen Ressourcen bereit und verfügbar?
  - Prozess

    - Wurden Prozesse und Verfahren eingehalten?
    - Waren Prozesse und Verfahren für diesen Vorfall bzw. für diese Art von Vorfall dokumentiert und verfügbar?
    - Fehlten erforderliche Prozesse und Verfahren?
    - Konnten die Notfallteams rechtzeitig auf die erforderlichen Informationen zugreifen, um auf das Problem zu reagieren?
  - Technologie
    - Haben die bestehenden Warnsysteme die Aktivität effektiv identifiziert und gemeldet?
    - Müssen bestehende Warnungen verbessert oder neue Warnungen für diesen Vorfall bzw. für diese Art von Vorfall erstellt werden?
    - Ermöglichen die vorhandenen Tools eine effektive Untersuchung (Suche/Analyse) des Vorfalls?
- Was kann getan werden, um diesen Vorfall bzw. diese Art von Vorfall früher zu erkennen?
- Was kann getan werden, um zu verhindern, dass sich dieser Vorfall bzw. diese Art von Vorfall wiederholt?
- Wer ist für den Verbesserungsplan zuständig und wie testen Sie, ob er implementiert wurde?
- Wie sieht der Zeitplan für die Implementierung und Erprobung der zusätzlichen monitoring/ preventative Kontrollen/Prozesse aus?

Diese Liste ist nicht vollständig. Sie soll als Ausgangspunkt dienen, um zu ermitteln, welche Anforderungen das Unternehmen und das Unternehmen haben und wie Sie diese analysieren können, um am effektivsten aus Vorfällen zu lernen und Ihre Sicherheitslage kontinuierlich zu verbessern. Am wichtigsten ist, damit zu beginnen und Erkenntnisse standardmäßig in Ihren Prozess zur Vorfallreaktion, in die Dokumentation und in die Erwartungen der Stakeholder zu integrieren.

Legen Sie Erfolgskennzahlen fest

Kennzahlen sind notwendig, um Ihre Fähigkeiten zur Reaktion auf Vorfälle effektiv zu messen, zu bewerten und zu verbessern. Ohne Kennzahlen gibt es keine Referenz, anhand derer Sie genau messen oder sogar identifizieren können, wie gut Ihr Unternehmen abschneidet (oder nicht). Es gibt einige Kennzahlen, die bei der Reaktion auf Vorfälle üblich sind. Sie sind ein guter Ausgangspunkt für ein Unternehmen, das Erwartungen und Referenzen für das Streben nach operativer Exzellenz ermitteln möchte.

Durchschnittliche Zeit bis zur Erkennung

Die durchschnittliche Erkennungszeit ist die durchschnittliche Zeit, die benötigt wird, um einen möglichen Sicherheitsvorfall zu entdecken. Konkret handelt es sich dabei um die Zeit zwischen dem Auftreten des ersten Bedrohungsindikators und der ersten Identifizierung oder Warnung.

Sie können diese Metrik verwenden, um zu verfolgen, wie effektiv Ihre Erkennungs- und Warnsysteme arbeiten. Effektive Erkennungs- und Warnmechanismen sind entscheidend, um sicherzustellen, dass sich mögliche Sicherheitsvorfälle nicht in Ihren Umgebungen fortsetzen.

Je länger die durchschnittliche Erkennungszeit ist, desto größer ist die Notwendigkeit, zusätzliche oder effektivere Warnmeldungen und Mechanismen zu entwickeln, um mögliche Sicherheitsvorfälle zu identifizieren und aufzudecken. Je kürzer die durchschnittliche Erkennungszeit ist, desto besser funktionieren Ihre Erkennungs- und Warnmechanismen.

Durchschnittliche Zeit bis zur Bestätigung

Die durchschnittliche Zeit bis zur Bestätigung ist die durchschnittliche Zeit, die benötigt wird, um einen möglichen Sicherheitsvorfall zu bestätigen und zu priorisieren. Konkret handelt es sich dabei um die Zeit zwischen der Generierung einer Warnung und der Identifizierung und Priorisierung der Warnung durch einen Mitarbeiter Ihres SOC oder Incident-Response-Teams, der die Warnung für die Bearbeitung identifiziert und priorisiert.

Mithilfe dieser Kennzahl können Sie nachverfolgen, wie gut Ihr Team Warnmeldungen verarbeitet und priorisiert. Wenn Ihr Team nicht in der Lage ist, Benachrichtigungen effektiv zu identifizieren und zu priorisieren, werden die Antworten verzögert und sind ineffektiv.

Je länger die durchschnittliche Zeit bis zur Bestätigung ist, desto größer ist die Notwendigkeit, sicherzustellen, dass Ihr Team sowohl über angemessene Ressourcen als auch über Schulungen verfügt, um einen möglichen Sicherheitsvorfall schnell zu erkennen und zu priorisieren, um darauf zu reagieren. Je kürzer die durchschnittliche Zeit bis zur Bestätigung ist, desto besser reagiert Ihr Team auf Sicherheitswarnungen und zeigt, dass es effektiv vorbereitet ist und in der Lage ist, sie gut zu priorisieren.

Durchschnittliche Reaktionszeit

Die durchschnittliche Reaktionszeit ist die durchschnittliche Zeit, die benötigt wird, um mit der ersten Reaktion auf einen möglichen Sicherheitsvorfall zu beginnen. Konkret handelt es sich dabei um die Zeit zwischen der ersten Warnung oder Entdeckung eines möglichen Sicherheitsvorfalls und den ersten Maßnahmen zur Reaktion darauf. Dies entspricht der mittleren Zeit bis zur Bestätigung,

ist jedoch die Messung bestimmter Reaktionsmaßnahmen (z. B. Erfassung von Systemdaten, Eindämmung des Systems) im Vergleich zur einfachen Erkennung oder Bestätigung der Situation.

Anhand dieser Kennzahl können Sie nachverfolgen, wie gut Sie auf Sicherheitsvorfälle vorbereitet sind. Wie bereits erwähnt, ist die Vorbereitung der Schlüssel zu einer effektiven Reaktion. Weitere Informationen finden Sie im the section called “Vorbereitung” Abschnitt dieses Dokuments.

Je länger die durchschnittliche Reaktionszeit ist, desto größer ist die Notwendigkeit, sicherzustellen, dass Ihr Team in der richtigen Vorgehensweise geschult ist, damit die Reaktionsprozesse effektiv dokumentiert und genutzt werden. Je kürzer die durchschnittliche Reaktionszeit ist, desto besser ist Ihr Team darin, eine angemessene Reaktion auf identifizierte Warnungen zu finden und die erforderlichen Reaktionsmaßnahmen zu ergreifen, um den Weg zurück zu einem sicheren Betrieb zu beginnen.

Durchschnittliche Eindämmungszeit

Die durchschnittliche Zeit bis zur Eindämmung ist die durchschnittliche Zeit, die benötigt wird, um einen möglichen Sicherheitsvorfall einzudämmen. Konkret handelt es sich dabei um die Zeit zwischen der ersten Warnung oder Entdeckung eines möglichen Sicherheitsvorfalls und dem Abschluss von Gegenmaßnahmen, die wirksam verhindern, dass der Angreifer oder die kompromittierten Systeme weiteren Schaden anrichten.

Anhand dieser Kennzahl können Sie nachverfolgen, wie gut Ihr Team in der Lage ist, mögliche Sicherheitsvorfälle einzudämmen oder einzudämmen. Die Unfähigkeit, mögliche Sicherheitsvorfälle schnell und effektiv einzudämmen, erhöht die Auswirkungen, den Umfang und die Gefahr, dass weitere Sicherheitsvorfälle gefährdet werden.

Je länger die durchschnittliche Eindämmungszeit ist, desto größer ist die Notwendigkeit, sowohl Wissen als auch Fähigkeiten aufzubauen, um die bei Ihnen auftretenden Sicherheitsvorfälle schnell und effektiv zu mindern und einzudämmen. Je kürzer die mittlere Eindämmungszeit ist, desto besser versteht Ihr Team die erforderlichen Maßnahmen zur Abwehr und Eindämmung identifizierter Bedrohungen und setzt sie um, um die Auswirkungen, den Umfang und die Risiken für das Unternehmen zu verringern.

Durchschnittliche Zeit bis zur Erholung

Die durchschnittliche Zeit bis zur Wiederherstellung ist die durchschnittliche Zeit, die benötigt wird, um den Betrieb nach einem möglichen Sicherheitsvorfall wieder vollständig wiederherzustellen. Konkret ist dies die Zeit zwischen der ersten Warnung oder der Entdeckung eines möglichen

Sicherheitsvorfalls und dem Zeitpunkt, zu dem das Unternehmen wieder normal und sicher arbeitet, ohne von dem Vorfall betroffen zu sein.

Anhand dieser Kennzahl können Sie nachverfolgen, wie effektiv Ihre Teams dabei sind, Systeme, Konten und Umgebungen nach einem Sicherheitsvorfall wieder in sicheren Betrieb zu versetzen. Die Unfähigkeit, schnell oder effektiv zu einem sicheren Betrieb zurückzukehren, kann sich nicht nur auf die Sicherheit auswirken, sondern auch die Auswirkungen und Kosten für das Unternehmen und seine Abläufe erhöhen.

Je länger die durchschnittliche Wiederherstellungszeit ist, desto größer ist die Notwendigkeit, Ihre Teams und Umgebungen darauf vorzubereiten, über die geeigneten Mechanismen (z. B. Failover-Prozesse und CI/CD Pipelines zur sicheren Neubereitstellung sauberer Systeme) zu verfügen, um die Auswirkungen von Sicherheitsvorfällen auf den Betrieb und das Unternehmen zu minimieren. Je kürzer die durchschnittliche Wiederherstellungszeit ist, desto effektiver können Ihre Teams die Auswirkungen von Sicherheitsvorfällen auf Ihren Betrieb und Ihr Geschäft minimieren.

Verweildauer des Angreifers

Die Verweildauer eines Angreifers ist die durchschnittliche Zeit, während der ein nicht autorisierter Benutzer Zugriff auf ein System oder eine Umgebung hat. Dies entspricht der durchschnittlichen Zeit bis zur Eindämmung, mit der Ausnahme, dass der Zeitraum mit dem Zeitpunkt beginnt, zu dem der Angreifer zum ersten Mal Zugriff auf das System oder die Umgebungen erlangt hat, was vor der ersten Warnung oder Entdeckung liegen kann.

Mit dieser Metrik können Sie verfolgen, wie gut viele Ihrer Systeme und Mechanismen zusammenarbeiten, um den Zeitaufwand, den Zugriff und die Möglichkeiten zu reduzieren, die ein Angreifer oder eine Bedrohung hat, Ihre Umgebung zu beeinträchtigen. Die Reduzierung der Verweildauer von Angreifern sollte für Ihre Teams und Ihr Unternehmen oberste Priorität haben.

Je länger die Verweildauer der Angreifer ist, desto wichtiger ist es, herauszufinden, welche Teile des Incident-Response-Prozesses verbessert werden müssen, um sicherzustellen, dass Ihre Teams in der Lage sind, die Auswirkungen und das Ausmaß von Bedrohungen oder Angriffen in Ihren Umgebungen zu minimieren. Je kürzer die Verweildauer der Angreifer ist, desto besser können Ihre Teams die Zeit und die Chancen minimieren, die eine Bedrohung oder ein Angreifer in Ihren Umgebungen hat, wodurch letztlich das Risiko und die Auswirkungen auf Ihren Betrieb und Ihr Geschäft reduziert werden.

Zusammenfassung der Kennzahlen

Durch die Festlegung und Nachverfolgung von Kennzahlen für die Reaktion auf Vorfälle können Sie Ihre Fähigkeiten zur Reaktion auf Vorfälle effektiv messen, bewerten und verbessern. Um dies zu erreichen, gibt es eine Reihe gängiger Kennzahlen zur Reaktion auf Vorfälle, die in diesem Abschnitt hervorgehoben wurden. In Tabelle 5 sind diese Kennzahlen zusammengefasst.

Tabelle 5 — Kennzahlen zur Reaktion auf Vorfälle

Metrik	Description
Durchschnittliche Erkennungszeit	Durchschnittliche Zeit, die zur Entdeckung eines möglichen Sicherheitsvorfalls benötigt wird
Durchschnittliche Zeit bis zur Bestätigung	Durchschnittliche Zeit, die benötigt wird, um einen möglichen Sicherheitsvorfall zu bestätige n (und zu priorisieren)
Durchschnittliche Reaktionszeit	Durchschnittliche Zeit, die benötigt wird, um mit der ersten Reaktion auf einen möglichen Sicherheitsvorfall zu beginnen
Durchschnittliche Zeit bis zur Eindämmung	Durchschnittliche Zeit, die benötigt wird, um einen möglichen Sicherheitsvorfall einzudämm en
Durchschnittliche Zeit bis zur Wiederherstellung	Durchschnittliche Zeit bis zur vollständigen Wiederherstellung des Betriebs nach einem möglichen Sicherheitsvorfall
Verweildauer des Angreifers	Durchschnittliche Zeit, in der ein Angreifer Zugriff auf ein System oder eine Umgebung hat

Verwenden Sie Kompromissindikatoren (IOCs)

Ein Indikator für eine Gefährdung (IOC) ist ein Artefakt, das in oder auf einem Netzwerk, System oder einer Umgebung beobachtet wird und das (mit einem hohen Maß an Sicherheit) böswillige Aktivitäten oder Sicherheitsvorfälle identifizieren kann. IOCs kann in einer Vielzahl von Formen existieren,

darunter IP-Adressen, Domänen, Artefakte auf Netzwerkebene wie TCP-Flags oder Payloads, Artefakte auf System- oder Host-Ebene wie ausführbare Dateien, Dateinamen und Hashes, Protokolldateieinträge oder Registrierungseinträge und mehr. Sie können auch eine Kombination von Elementen oder Aktivitäten sein, z. B. das Vorhandensein bestimmter Elemente oder Artefakte auf einem System (eine bestimmte Datei oder Gruppe von Dateien und Registrierungselementen), Aktionen, die in einer bestimmten Reihenfolge ausgeführt werden (eine Anmeldung bei einem System von einer bestimmten IP aus, gefolgt von bestimmten anomalen Befehlen) oder Netzwerkaktivität (anomaler eingehender oder ausgehender Verkehr zu oder von bestimmten Domänen), die auf eine bestimmte Bedrohungs-, Angriffs- oder Angriffsmethode hinweisen können.

Während Sie daran arbeiten, Ihr Incident-Response-Programm schrittweise zu verbessern, sollten Sie ein Framework zur Erfassung, Verwaltung und Nutzung IOCs als Mechanismus implementieren, um Erkennungen und Warnmeldungen kontinuierlich aufzubauen und zu verbessern und die Geschwindigkeit und Effizienz von Untersuchungen zu verbessern. Sie können damit beginnen, die Erfassung und Verwaltung von Daten IOCs in die Analyse- und Untersuchungsphasen Ihrer Prozesse zur Reaktion auf Vorfälle zu integrieren. Durch proaktives Identifizieren, Sammeln und Speichern IOCs als Standardbestandteil Ihres Prozesses können Sie ein Datenarchiv (als Teil eines umfassenderen Threat-Intelligence-Programms) aufbauen, das wiederum verwendet werden kann, um bestehende Erkennungen und Warnungen zu verbessern, zusätzliche Erkennungen und Warnungen zu erstellen, zu ermitteln, wo und wann ein Artefakt zuvor entdeckt wurde, und Dokumentationen darüber zu erstellen und zu referenzieren, wie Untersuchungen zuvor durchgeführt wurden IOCs, einschließlich Abgleich und mehr.

Kontinuierliche Aus- und Weiterbildung

Allgemeine und berufliche Bildung sind sowohl sich weiterentwickelnde als auch kontinuierliche Anstrengungen, die zielgerichtet fortgeführt und fortgeführt werden sollten. Es gibt eine Vielzahl von Mechanismen, mit denen überprüft werden kann, ob Ihr Team das Bewusstsein, das Wissen und die Fähigkeiten bewahrt, die dem sich entwickelnden Stand der Technik und der Bedrohungslandschaft angemessen sind.

Ein Mechanismus besteht darin, Weiterbildung als Standardbestandteil der Ziele und Abläufe Ihrer Teams einzusetzen. Wie im Abschnitt Vorbereitung erwähnt, müssen Ihre Mitarbeiter und Beteiligten bei der Reaktion auf Vorfälle effektiv darin geschult werden, interne AWS Vorfälle zu erkennen, darauf zu reagieren und zu untersuchen. Bildung ist jedoch kein einmaliges Unterfangen. Die Schulung muss kontinuierlich fortgesetzt werden, um sicherzustellen, dass Ihr Team stets über die neuesten technologischen Fortschritte, Aktualisierungen und Verbesserungen informiert ist, die zur Verbesserung der Wirksamkeit und Effizienz der Reaktion genutzt werden können, sowie über

Ergänzungen oder Aktualisierungen von Daten, die zur Verbesserung von Untersuchungen und Analysen genutzt werden können.

Ein weiterer Mechanismus besteht darin, zu überprüfen, ob Simulationen regelmäßig (z. B. vierteljährlich) durchgeführt werden und sich auf spezifische Ergebnisse für das Unternehmen konzentrieren. Weitere Informationen finden Sie im the section called “Führen Sie regelmäßige Simulationen durch” Abschnitt dieses Dokuments.

Die Durchführung von ersten Übungen am Tisch ist zwar eine hervorragende Möglichkeit, eine erste Grundlage für Verbesserungen zu schaffen, aber kontinuierliche Tests sind der Schlüssel zu nachhaltigen Verbesserungen und zur Aufrechterhaltung eines up-to-date genauen Abbilds des aktuellen Betriebszustands. Testen Sie anhand der neuesten und kritischsten Sicherheitssituationen und der wichtigsten oder neuesten Reaktionsmöglichkeiten und lassen Sie die gewonnenen Erkenntnisse in die Ausbildung und processes/procedures den Betrieb einfließen, um sicherzustellen, dass Sie in der Lage sind, Ihre Reaktionsprozesse und Ihr Programm insgesamt kontinuierlich zu verbessern.

Schlussfolgerung

Wenn Sie Ihre Reise in die Cloud fortsetzen, ist es wichtig, dass Sie die grundlegenden Konzepte zur Reaktion auf Sicherheitsvorfälle für Ihre AWS Umgebung berücksichtigen. Sie können die verfügbaren Kontrollen, Cloud-Funktionen und Behebungsoptionen kombinieren, um die Sicherheit Ihrer Cloud-Umgebung zu verbessern. Sie können auch klein anfangen und schrittweise Automatisierungsfunktionen einführen, die Ihre Reaktionsgeschwindigkeit verbessern, sodass Sie besser auf Sicherheitsereignisse vorbereitet sind.

Mitwirkende

Zu den aktuellen und früheren Mitwirkenden an diesem Dokument gehören:

- Anna McAbee, leitende Architektin für Sicherheitslösungen, Amazon Web Services
- Freddy Kasprzykowski, leitender Sicherheitsberater, Amazon Web Services
- Jason Hurst, leitender Sicherheitsingenieur, Amazon Web Services
- Jonathon Poling, Hauptsicherheitsberater, Amazon Web Services
- Josh Du Lac, Senior Manager, Sicherheitslösungsarchitektur, Amazon Web Services
- Paco Hope, leitender Sicherheitsingenieur, Amazon Web Services

- Ryan Tick, leitender Sicherheitsingenieur, Amazon Web Services
- Steve de Vera, leitender Sicherheitsingenieur, Amazon Web Services

Anhang A: Definitionen der Cloud-Funktionen

AWS bietet über 200 Cloud-Dienste und Tausende von Funktionen. Viele von ihnen bieten native Erkennungs-, Präventions- und Reaktionsfunktionen, und andere können zur Entwicklung maßgeschneiderter Sicherheitslösungen verwendet werden. Dieser Abschnitt enthält eine Untergruppe der Dienste, die für die Reaktion auf Vorfälle in der Cloud am relevantesten sind.

Themen

Protokollierung und Ereignisse

AWS CloudTrail— AWS CloudTrail Service, der die Unternehmensführung, die Einhaltung von Vorschriften, die betriebliche Prüfung und die Risikoprüfung von AWS Konten ermöglicht. Mit CloudTrail können Sie Kontoaktivitäten im Zusammenhang mit Aktionen AWS dienstübergreifend protokollieren, kontinuierlich überwachen und speichern. CloudTrail bietet einen Ereignisverlauf Ihrer AWS Kontoaktivitäten, einschließlich Aktionen, die über die AWS-Managementkonsole Befehlszeilentools, und andere AWS Dienste ausgeführt wurden. AWS SDKs Dieser Ereignisverlauf vereinfacht die Sicherheitsanalyse, die Nachverfolgung von Ressourcenänderungen und die Fehlerbehebung. CloudTrail protokolliert zwei verschiedene Arten von AWS API-Aktionen:

- CloudTrail Verwaltungsereignisse (auch als Operationen auf Steuerungsebene bezeichnet) zeigen Verwaltungsvorgänge, die mit Ressourcen in Ihrem AWS Konto ausgeführt werden. Dazu gehören Aktionen wie das Erstellen eines Amazon S3 S3-Buckets und das Einrichten der Protokollierung.
- CloudTrail Datenereignisse (auch bekannt als Datenebenenoperationen) zeigen die Ressourcenoperationen, die auf oder innerhalb einer Ressource in Ihrem AWS Konto ausgeführt wurden. Bei diesen Vorgängen handelt es sich häufig um umfangreiche Aktivitäten. Dazu gehören Aktionen wie API-Aktivitäten auf Amazon S3 S3-Objektebene (z. B., `GetObject` `DeleteObject`, und `PutObject` API-Operationen) und Lambda-Funktionsaufrufaktivitäten.

AWS Config— AWS Config ist ein Service, mit dem Kunden die Konfigurationen Ihrer Ressourcen bewerten, prüfen und bewerten können. AWS AWS Config überwacht und zeichnet Ihre AWS Ressourcenkonfigurationen kontinuierlich auf und ermöglicht es Ihnen, die Auswertung der aufgezeichneten Konfigurationen anhand der gewünschten Konfigurationen zu automatisieren. Mit AWS Config dieser Funktion können Kunden manuell oder automatisch Änderungen an Konfigurationen und Beziehungen zwischen AWS Ressourcen überprüfen, den Verlauf der Ressourcenkonfiguration detailliert nachverfolgen und die allgemeine Konformität mit den in den Kundenrichtlinien angegebenen Konfigurationen ermitteln. Dies ermöglicht eine Vereinfachung von Compliance-Prüfungen, Sicherheitsanalysen, Änderungsmanagement und betrieblicher Fehlerbehebung.

Amazon EventBridge — Amazon EventBridge liefert nahezu in Echtzeit einen Stream von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben oder wann API-Aufrufe von veröffentlicht werden AWS CloudTrail. Mithilfe einfacher Regeln, die Sie schnell einrichten können, können Sie Ereignisse zuordnen und sie an eine oder mehrere Zielfunktionen oder Streams weiterleiten. EventBridge wird sich betrieblicher Änderungen bewusst, sobald sie auftreten. EventBridge kann auf diese betrieblichen Änderungen reagieren und bei Bedarf Korrekturmaßnahmen ergreifen, indem es Nachrichten sendet, um auf die Umgebung zu reagieren, Funktionen aktiviert, Änderungen vornimmt und Statusinformationen erfasst. Einige Sicherheitsdienste, wie Amazon GuardDuty, produzieren ihre Ergebnisse in Form von EventBridge Ereignissen. Viele Sicherheitsdienste bieten auch die Möglichkeit, ihre Ausgaben an Amazon S3 zu senden.

Amazon S3 S3-Zugriffsprotokolle — Wenn vertrauliche Informationen in einem Amazon S3 S3-Bucket gespeichert sind, können Kunden Amazon S3 S3-Zugriffsprotokolle aktivieren, um jeden Upload, Download und jede Änderung dieser Daten aufzuzeichnen. Dieses Protokoll ist unabhängig von den CloudTrail Protokollen, die Änderungen am Bucket selbst aufzeichnen (z. B. geänderte Zugriffs- und Lebenszyklusrichtlinien), und zusätzlich zu diesen Protokollen. Es sei darauf hingewiesen, dass die Aufzeichnungen der Zugriffsprotokolle nach bestem Wissen und Gewissen übermittelt werden. Die meisten Anforderungen nach einem Bucket, der für die Protokollierung richtig konfiguriert ist, führen zu einem ausgelieferten Protokollsatz. Die Vollständigkeit und Aktualität der Serverprotokollierung wird nicht garantiert.

Amazon CloudWatch Logs — Kunden können Amazon CloudWatch Logs verwenden, um Protokolldateien zu überwachen, zu speichern und darauf zuzugreifen, die von Betriebssystemen, Anwendungen und anderen Quellen stammen, die in Amazon EC2 EC2-Instances mit einem CloudWatch Logs-Agenten ausgeführt werden. CloudWatch Protokolle können ein Ziel für Route

53-DNS-Abfragen AWS CloudTrail, VPC-Flow-Logs, Lambda-Funktionen und andere sein. Kunden können dann die zugehörigen Protokolldaten aus CloudWatch Logs abrufen.

Amazon VPC Flow Logs — VPC Flow Logs ermöglicht es Kunden, Informationen über IP-Verkehr zu und von Netzwerkschnittstellen in VPCs zu erfassen. Nach der Aktivierung von Flow-Logs können sie zu Amazon CloudWatch Logs und Amazon S3 gestreamt werden. VPC Flow Logs unterstützt Kunden bei einer Reihe von Aufgaben wie der Behebung von Problemen, warum bestimmter Datenverkehr eine Instance nicht erreicht, der Diagnose zu restriktiver Sicherheitsgruppenregeln und der Verwendung als Sicherheitstool zur Überwachung des Datenverkehrs zu EC2-Instances. Verwenden Sie die aktuellste Version der VPC-Flow-Protokollierung, um die robustesten Felder zu erhalten.

AWS WAF Protokolle — AWS WAF unterstützt die vollständige Protokollierung aller vom Service überprüften Webanfragen. Kunden können diese in Amazon S3 speichern, um Konformitäts- und Prüfanforderungen sowie Debugging und Forensik zu erfüllen. Diese Protokolle helfen Kunden dabei, die Hauptursache für initiierte Regeln und blockierte Webanfragen zu ermitteln. Protokolle können in SIEM- und Protokollanalysetools von Drittanbietern integriert werden.

Route 53 Resolver-Abfrageprotokolle — Mit Route 53 Resolver-Abfrageprotokollen können Sie alle DNS-Abfragen protokollieren, die von Ressourcen innerhalb von Amazon Virtual Private Cloud (Amazon VPC) gestellt wurden. Ganz gleich, ob es sich um eine Amazon EC2 EC2-Instance, eine AWS Lambda Funktion oder einen Container handelt: Wenn sie sich in Ihrer Amazon VPC befindet und eine DNS-Abfrage durchführt, protokolliert diese Funktion diese. Sie können dann untersuchen und besser verstehen, wie Ihre Anwendungen funktionieren.

Andere AWS Protokolle — veröffentlicht AWS kontinuierlich Servicefunktionen und Funktionen für Kunden mit neuen Protokollierungs- und Überwachungsfunktionen. Informationen zu den Funktionen, die für die einzelnen AWS Dienste verfügbar sind, finden Sie in unserer öffentlichen Dokumentation.

Sichtbarkeit und Alarmierung

AWS Security Incident Response— AWS Security Incident Response ist ein umfassender Service, der Unternehmen bei der Bewältigung von Sicherheitsereignissen während ihres gesamten Lebenszyklus unterstützt, indem automatisierte Funktionen mit fachkundiger menschlicher Unterstützung kombiniert werden. Der Service nutzt automatisierte Überwachungs- und Ermittlungsfunktionen, um organisatorische Ressourcen freizusetzen und gleichzeitig eine wachsame Sicherheitsaufsicht aufrechtzuerhalten. Wenn Sicherheitsereignisse auftreten, ermöglicht er eine beschleunigte Kommunikation und Koordination zwischen den Beteiligten und sorgt so für schnelle Reaktionszeiten. Der Service unterstützt mehrere Anwendungsfälle, darunter die Vorbereitung

und Simulation von Sicherheitsereignissen, die Reaktion auf aktive Vorfälle und eine optimierte Berichterstattung und Analyse nach einem Vorfall. Dadurch wird sichergestellt, dass Unternehmen für die Bewältigung von Sicherheitsherausforderungen in jeder Phase gerüstet sind.

AWS Security Hub CSPM— AWS Security Hub CSPM bietet Kunden einen umfassenden Überblick über Sicherheitswarnungen mit hoher Priorität und den kontoübergreifenden Compliance-Status. AWS Security Hub CSPM aggregiert, organisiert und priorisiert Bedrohungserkenntnisse von AWS Diensten wie Amazon GuardDuty, Amazon Inspector, Amazon Macie und Lösungen. AWS Partner Die Ergebnisse werden auf integrierten Dashboards mit verwertbaren Grafiken und Tabellen visuell zusammengefasst. Sie können Ihre Umgebung auch kontinuierlich überwachen, indem Sie automatisierte Konformitätsprüfungen verwenden, die auf den AWS bewährten Verfahren und Industriestandards basieren, die Ihr Unternehmen befolgt.

Amazon GuardDuty — Amazon GuardDuty ist ein verwalteter Dienst zur Bedrohungserkennung, der kontinuierlich bösartiges oder unbefugtes Verhalten überwacht, um Kunden beim Schutz von AWS Konten und Workloads zu unterstützen. Es überwacht Aktivitäten wie ungewöhnliche API-Aufrufe oder potenziell nicht autorisierte Bereitstellungen, die auf eine mögliche Konto- oder Ressourcenkompromittierung von Amazon EC2 EC2-Instances, Amazon S3 S3-Buckets oder Aufklärungen durch böswillige Akteure hinweisen.

GuardDuty identifiziert mutmaßliche böswillige Akteure mithilfe integrierter Threat-Intelligence-Feeds mithilfe von maschinellem Lernen, um Anomalien bei der Konto- und Workload-Aktivität zu erkennen. Wenn eine potenzielle Bedrohung erkannt wird, sendet der Service eine detaillierte Sicherheitswarnung an die GuardDuty Konsole und CloudWatch an Ereignisse. Dadurch sind Warnmeldungen umsetzbar und lassen sich einfach in bestehende Eventmanagement- und Workflow-Systeme integrieren.

GuardDuty bietet außerdem zwei Add-Ons zur Überwachung auf Bedrohungen mit bestimmten Diensten: Amazon GuardDuty für Amazon S3 S3-Schutz und Amazon GuardDuty für Amazon EKS-Schutz. Der Amazon S3 S3-Schutz ermöglicht GuardDuty die Überwachung von API-Vorgängen auf Objektebene, um potenzielle Sicherheitsrisiken für Daten in Amazon S3 S3-Buckets zu identifizieren. Der Kubernetes-Schutz ermöglicht GuardDuty die Erkennung verdächtiger Aktivitäten und potenzieller Beeinträchtigungen von Kubernetes-Clustern innerhalb von Amazon EKS.

Amazon Macie — Amazon Macie ist ein KI-gestützter Sicherheitsservice, der Datenverlust verhindert, indem er sensible Daten, die in gespeichert sind, automatisch erkennt, klassifiziert und schützt. AWS Macie verwendet maschinelles Lernen (ML), um sensible Daten wie personenbezogene Daten (PII) oder geistiges Eigentum zu erkennen, einen Geschäftswert zuzuweisen und Transparenz darüber zu bieten, wo diese Daten gespeichert sind und wie sie in Ihrem Unternehmen verwendet werden.

Amazon Macie überwacht kontinuierlich die Datenzugriffsaktivitäten auf Anomalien und sendet Warnmeldungen, wenn das Risiko eines unbefugten Zugriffs oder unbeabsichtigter Datenlecks erkannt wird.

AWS-Config-Regeln— Eine AWS Config Regel stellt die bevorzugten Konfigurationen für eine Ressource dar und wird anhand von Konfigurationsänderungen an den entsprechenden Ressourcen bewertet, wie sie von aufgezeichnet wurden. AWS Config Sie können die Ergebnisse der Auswertung einer Regel anhand der Konfiguration einer Ressource in einem Dashboard sehen. Mithilfe von AWS Config Regeln können Sie Ihren allgemeinen Konformitäts- und Risikostatus aus Sicht der Konfiguration beurteilen, Konformitätstrends im Zeitverlauf anzeigen und herausfinden, welche Konfigurationsänderung dazu geführt hat, dass eine Ressource nicht mit einer Regel konform war.

AWS Trusted Advisor— AWS Trusted Advisor ist eine Online-Ressource, die Ihnen hilft, durch die Optimierung Ihrer AWS Umgebung Kosten zu senken, die Leistung zu steigern und die Sicherheit zu verbessern. Trusted Advisor bietet Anleitungen in Echtzeit, um Sie bei der Bereitstellung Ihrer Ressourcen zu unterstützen und dabei AWS bewährte Methoden zu befolgen. Alle Trusted Advisor Prüfungen, einschließlich der Integration von CloudWatch Ereignissen, stehen Kunden mit Business- und Enterprise Support-Plänen zur Verfügung.

Amazon CloudWatch — Amazon CloudWatch ist ein Überwachungsdienst für AWS Cloud Ressourcen und Anwendungen, auf denen Sie laufen AWS. Sie können CloudWatch damit Metriken sammeln und verfolgen, Protokolldateien sammeln und überwachen, Alarme einrichten und automatisch auf Änderungen Ihrer AWS Ressourcen reagieren. CloudWatch kann AWS Ressourcen wie Amazon EC2-Instances, Amazon DynamoDB-Tabellen und Amazon RDS-DB-Instances sowie von Ihren Anwendungen und Services generierte benutzerdefinierte Metriken und alle von Ihren Anwendungen generierten Protokolldateien überwachen. Sie können Amazon verwenden CloudWatch , um systemweite Einblicke in die Ressourcennutzung, die Anwendungsleistung und den Betriebszustand zu erhalten. Sie können diese Erkenntnisse nutzen, um entsprechend zu reagieren und dafür zu sorgen, dass Ihre Anwendung reibungslos läuft.

Amazon Inspector — Amazon Inspector ist ein automatisierter Sicherheitsbewertungsservice, der dazu beiträgt, die Sicherheit und Konformität von Anwendungen zu verbessern, auf denen bereitgestellt wird AWS. Amazon Inspector bewertet automatisch Schwachstellen in Anwendungen sowie Abweichungen von bewährten Methoden. Nach der Durchführung einer Bewertung erstellt Amazon Inspector eine detaillierte Liste der Sicherheitsfeststellungen, die nach Schweregrad priorisiert sind. Diese Ergebnisse können direkt oder als Teil detaillierter Bewertungsberichte überprüft werden, die über die Amazon Inspector Inspector-Konsole oder API verfügbar sind.

Amazon Detective — Amazon Detective ist ein Sicherheitsservice, der automatisch Protokolldaten aus Ihren AWS Ressourcen sammelt und mithilfe von maschinellem Lernen, statistischer Analyse und Graphentheorie einen verknüpften Datensatz erstellt, mit dem Sie schnellere und effizientere Sicherheitsuntersuchungen durchführen können. Detective kann Billionen von Ereignissen aus mehreren Datenquellen wie VPC Flow Logs usw. analysieren und GuardDuty erstellt automatisch eine einheitliche, interaktive Ansicht Ihrer Ressourcen, Benutzer und der Interaktionen zwischen ihnen im Laufe der Zeit. CloudTrail Mit dieser einheitlichen Ansicht können Sie alle Details und den Kontext an einem Ort visualisieren, um die zugrunde liegenden Gründe für die Ergebnisse zu ermitteln, relevante historische Aktivitäten aufzuschlüsseln und schnell die Ursache zu ermitteln.

-Automatisierung

AWS Lambda— AWS Lambda ist ein serverloser Rechendienst, der Ihren Code als Reaktion auf Ereignisse ausführt und die zugrunde liegenden Rechenressourcen automatisch für Sie verwaltet. Sie können Lambda verwenden, um andere AWS Dienste mit benutzerdefinierter Logik zu erweitern, oder Ihre eigenen Backend-Services erstellen, die AWS skalierbar, leistungsstark und sicher arbeiten. Lambda führt Ihren Code auf einer hochverfügbaren Recheninfrastruktur aus und führt die Verwaltung der Rechenressourcen für Sie durch. Dazu gehören Server- und Betriebssystemwartung, Kapazitätsbereitstellung und automatische Skalierung, Bereitstellung von Code- und Sicherheitspatches sowie Codeüberwachung und -protokollierung. Sie müssen lediglich den Code angeben.

AWS Step Functions— AWS Step Functions macht es einfach, die Komponenten verteilter Anwendungen und Microservices mithilfe visueller Workflows zu koordinieren. Step Functions bietet eine grafische Konsole, mit der Sie die Komponenten Ihrer Anwendung in einer Reihe von Schritten anordnen und visualisieren können. Dies macht es einfach, mehrstufige Anwendungen zu erstellen und auszuführen. Step Functions startet und verfolgt jeden Schritt automatisch und versucht es erneut, wenn Fehler auftreten, sodass Ihre Anwendung ordnungsgemäß und wie erwartet ausgeführt wird.

Step Functions protokolliert den Status jedes Schritts, sodass Sie Probleme schnell diagnostizieren und debuggen können, wenn etwas schief geht. Sie können Schritte ändern und hinzufügen, ohne Code schreiben zu müssen, sodass Sie Ihre Anwendung weiterentwickeln und schneller innovieren können. AWS Step Functions ist Teil von AWS Serverless und macht es einfach, AWS Lambda Funktionen für serverlose Anwendungen zu orchestrieren. Sie können Step Functions auch für die Microservices-Orchestrierung mithilfe von Rechenressourcen wie Amazon EC2 und Amazon ECS verwenden.

AWS Systems Manager — AWS Systems Manager bietet Ihnen Transparenz und Kontrolle über Ihre Infrastruktur AWS. Systems Manager bietet eine einheitliche Benutzeroberfläche, über die Sie Betriebsdaten von mehreren AWS Diensten anzeigen können, und ermöglicht es Ihnen, betriebliche Aufgaben AWS ressourcenübergreifend zu automatisieren. Mit Systems Manager können Sie Ressourcen nach Anwendungen gruppieren, Betriebsdaten zur Überwachung und Fehlerbehebung anzeigen und auf Ihre Ressourcengruppen reagieren. Systems Manager kann Ihre Instanzen in ihrem definierten Zustand halten, bei Bedarf Änderungen vornehmen, z. B. Anwendungen aktualisieren oder Shell-Skripts ausführen, und andere Automatisierungs- und Patchaufgaben ausführen.

Sicherer Speicher

Amazon Simple Storage Service — Amazon S3 ist ein Objektspeicher, der darauf ausgelegt ist, beliebige Datenmengen von überall zu speichern und abzurufen. Er ist auf eine Beständigkeit von 99,999999999% ausgelegt und speichert Daten für Millionen von Anwendungen, die von Marktführern in allen Branchen verwendet werden. Amazon S3 bietet umfassende Sicherheit und wurde entwickelt, um Sie bei der Erfüllung Ihrer gesetzlichen Anforderungen zu unterstützen. Es bietet Kunden Flexibilität bei den Methoden, die sie zur Datenverwaltung zur Kostenoptimierung, Zugriffskontrolle und Einhaltung von Vorschriften verwenden. Amazon S3 bietet query-in-place Funktionen, mit denen Sie leistungsstarke Analysen direkt für Ihre in Amazon S3 gespeicherten Daten ausführen können. Amazon S3 ist ein stark unterstützter Cloud-Speicherservice, der von einer der größten Communitys von Drittanbieterlösungen, Systemintegrator-Partnern und anderen AWS Diensten integriert wird.

Amazon Glacier — Amazon Glacier ist ein sicherer, langlebiger und extrem kostengünstiger Cloud-Speicherservice für Datenarchivierung und Langzeitsicherung. Er ist auf eine Beständigkeit von 99,999999999% ausgelegt, bietet umfassende Sicherheit und wurde entwickelt, um Sie bei der Erfüllung Ihrer gesetzlichen Anforderungen zu unterstützen. Amazon Glacier bietet query-in-place Funktionen, mit denen Sie leistungsstarke Analysen direkt für Ihre Archivdaten im Ruhezustand ausführen können. Um die Kosten niedrig zu halten und dennoch für unterschiedliche Abrufanforderungen geeignet zu sein, bietet Amazon Glacier drei Optionen für den Zugriff auf Archive, von wenigen Minuten bis zu mehreren Stunden.

Künftige und maßgeschneiderte Sicherheitsfunktionen

Die oben genannten Dienste und Funktionen stellen keine vollständige Liste dar. AWS fügt ständig neue Funktionen hinzu. Weitere Informationen finden Sie auf den Seiten Was ist neu bei AWS und AWS Cloud Security. Zusätzlich zu den Sicherheitsdiensten, die als native Cloud-Dienste AWS angeboten werden, könnten Sie daran interessiert sein, Ihre eigenen Funktionen zusätzlich zu den AWS Diensten aufzubauen.

Wir empfehlen zwar, einige grundlegende Sicherheitsdienste in Ihren Konten zu aktivieren, z. B. AWS CloudTrail Amazon und Amazon Macie GuardDuty, aber Sie möchten diese Funktionen möglicherweise erweitern, um zusätzlichen Nutzen aus Ihren Protokollbeständen zu ziehen. Es gibt eine Reihe von Partner-Tools, die beispielsweise in unserem APN-Sicherheitskompetenzprogramm aufgeführt sind. Möglicherweise möchten Sie auch Ihre eigenen Abfragen schreiben, um Ihre Logs zu durchsuchen. Mit der großen Anzahl an verwalteten Diensten, die das AWS Unternehmen anbietet, war dies noch nie so einfach. Es gibt viele zusätzliche AWS Dienste, die Sie bei Untersuchungen unterstützen können, die nicht in diesem paper behandelt werden, z. B. Amazon Athena, Amazon OpenSearch Service, Amazon Quick, Amazon Machine Learning und Amazon EMR.

Anhang B: Ressourcen zur Reaktion auf AWS Vorfälle

AWS veröffentlicht Ressourcen, um Kunden bei der Entwicklung von Funktionen zur Reaktion auf Vorfälle zu unterstützen. Die meisten Beispielcodes und Verfahren finden Sie im AWS externen GitHub öffentlichen Repository. Im Folgenden finden Sie einige Ressourcen, die Beispiele für die Reaktion auf Vorfälle enthalten.

Ressourcen aus dem Playbook

- Framework for Incident Response Playbooks — Ein Beispiel-Framework, mit dem Kunden Sicherheitsplaybooks erstellen, entwickeln und integrieren können, um sich auf mögliche Angriffsszenarien bei der Nutzung von Diensten vorzubereiten. AWS
- Beispiele für Incident Response Playbooks — Playbooks zu gängigen Szenarien, mit denen Kunden konfrontiert sind. AWS
- AWS kündigt die Veröffentlichung von fünf öffentlich zugänglichen Workshops an.

Forensische Ressourcen

- Automatisiertes Framework zur Reaktion auf Vorfälle und Forensik — Dieses Framework und die Lösung bieten einen standardmäßigen digitalen forensischen Prozess, der aus den folgenden Phasen besteht: Eindämmung, Erfassung, Untersuchung und Analyse. Es nutzt die Funktionen von AWS Λ, um den Incident-Response-Prozess automatisiert und wiederholbar auszulösen. Es ermöglicht die Trennung von Konten, um die Automatisierungsschritte durchzuführen, Artefakte zu speichern und forensische Umgebungen zu erstellen.
- Automated Forensics Orchestrator für Amazon EC2 — Dieser Implementierungsleitfaden bietet eine Self-Service-Lösung zur Erfassung und Untersuchung von Daten aus EC2-Instances und

angehängten Volumes für forensische Analysen, falls ein potenzielles Sicherheitsproblem entdeckt wird. Es gibt eine Vorlage für die Bereitstellung der Lösung. AWS CloudFormation

- So automatisieren Sie die forensische Erfassung von Festplatten in AWS— In diesem AWS Blog wird beschrieben, wie Sie einen Automatisierungsworkflow einrichten, um die Festplattennachweise für die Analyse zu erfassen und so den Umfang und die Auswirkungen potenzieller Sicherheitsvorfälle zu ermitteln. Es ist auch eine AWS CloudFormation Vorlage für die Bereitstellung der Lösung enthalten.

Hinweise

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

© 2024 Amazon Web Services, Inc. oder seine Tochtergesellschaften. Alle Rechte vorbehalten.

Dokumentverlauf

In der folgenden Tabelle werden wichtige Ergänzungen der Dokumentation zur Reaktion auf AWS Sicherheitsvorfälle ab dem 1. Januar 2026 beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie den RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Aktualisieren Sie die Richtlinienbeschreibung für die Rollenrichtlinie „ AWS Security Incident Response Triage Service“	Aktualisieren Sie die Richtlinienbeschreibung für die Service-Rollenrichtlinie „ AWS Security Incident Response Triage“, um den Änderungen Rechnung zu tragen, die es dem Dienst ermöglichen, die Serviceoptimierung zu verbessern und Informationen zur Untersuchung potenzieller Vorfälle zu sammeln.	27. März 2026
Metadaten einreichen	Es wurden Anweisungen zum Einreichen von Metadaten anhand von AWS Support Fällen hinzugefügt.	27. März 2026
Reichen Sie Ihre Containment-Einstellungen ein	Es wurden Anweisungen zum Einreichen von Containment-Präferenzen über AWS Support Fälle hinzugefügt.	27. März 2026
Vorlage für die Eindämmung StackSet	Die StackSet CloudFormation Containment-Vorlage wurde aktualisiert.	27. März 2026
Die AWS-Region Überlegungen zu delegierten Administratorkonten wurden geklärt	Es wurde klargestellt, dass Sie bei der Ersteinrichtung zwar ein delegiertes AWS Security Incident Response-	20. März 2026

	Administratorkonto in einem AWS-Region Konto angeben, der Service jedoch unternehmensweite Abdeckung für alle unterstützten Konten bietet. AWS-Regionen	
Definieren Sie die Einstellungen für Eindämmungsmaßnahmen	Der Abschnitt mit den Einstellungen für Eindämmungsaktionen wurde aktualisiert, sodass er den aktuellen Optionen entspricht.	19. März 2026
Proaktive Reaktion und Alert-Triaging	Verweise darauf, dass der Workflow für proaktive Reaktion und Alert-Triaging optional ist, wurden entfernt.	3. März 2026
Zeitplan für die Antwort	Der Antwortzeitplan wurde aktualisiert und gibt nun 15 Minuten SLO für die Bestätigung des Falls und 5 Arbeitstage für die Kundenantwort vor Abschluss des Falls an.	24. Februar 2026
Bewährte Methoden für die Kommunikation	Der Zeitplan für den Abschluss von Fällen wurde aktualisiert und legt nun 5 Arbeitstage für die Beantwortung kritischer Informationsanfragen durch den Kunden fest.	24. Februar 2026
AWS CLI Die Referenz wurde in Interaction with Security Incident Response hinzugefügt mit AWS CloudShell	Link zur AWS Command Line Interface Referenz für die Reaktion auf AWS Sicherheitsvorfälle hinzugefügt.	24. Februar 2026

RACI-Matrix	In der RACI-Matrix wurde „CIRT-Eindämmungsaktionen autorisieren“ auf „Eindämmungsaktionen autorisieren“ aktualisiert.	13. Februar 2026
Einstellungen für Containment	Die Einstellungsoptionen für Eindämmungen wurden von „Keine Eindämmungsmaßnahmen“, „Eindämmung mit Genehmigung“ und „Automatische Eindämmung“ auf „Genehmigung erforderlich“, „Enthalten bestätigt“ und „Verdächtigen enthalten“ mit überarbeiteten Beschreibungen aktualisiert.	13. Februar 2026
Reaktion auf Sicherheitsvorfälle nach der Bereitstellung	Link zur Demo „Reaktion auf AWS Sicherheitsvorfälle: Neue Integrationen und Abonnements auf OU-Ebene“ hinzugefügt.	4. Februar 2026
Überwachung und Untersuchung	Den Intro- und Unterabschnitten auf dieser Seite wurden überarbeitete Inhalte hinzugefügt.	4. Februar 2026
Erkennen und Analysieren	Der Einführung und den Unterabschnitten auf dieser Seite wurden überarbeitete Inhalte hinzugefügt.	4. Februar 2026
Enthalten	Überarbeiteter Inhalt zu dieser Seite hinzugefügt.	4. Februar 2026

KI-Ermittlungsagent	Dieser Seite wurde ein Haftungsausschluss zur Verwendung von Kundendaten hinzugefügt. Haftungsausschluss: AI Investigative Agent verwendet keine Kundendaten für Modellschulungen und gibt Kundendaten nicht an Dritte weiter.	4. Februar 2026

Änderungen	Beschreibung	Date
Mitgliedschaft kündigen	Die Seite zur Kündigung der Mitgliedschaft wurde aktualisiert, um darauf hinzuweisen, dass die Mitgliedschaft und der Service sofort nach der Kündigung enden und nicht mit dem Ende des Abrechnungszeitraums.	20. November 2025
AWS Verwaltete Richtlinien	Zur Liste der Aktionen, die der Service anbietet, wurden Fälle aktualisieren, Fallkommentare erstellen, Fälle auflisten und Kommentare zu Fällen auflisten hinzugefügt.	19. November 2025
Verwenden von servicegebundenen Rollen	Zur Liste der Aktionen, die der Service anbietet, wurden Fälle aktualisieren, Fallkommentare erstellen, Fälle auflisten und Kommentare zu Fällen auflisten hinzugefügt.	19. November 2025

Änderungen	Beschreibung	Date
Kommunikationspräferenzen	Der Abschnitt Kommunikationseinstellungen wurde für die Dokumentation neuer Funktionen erstellt und aktualisiert.	12. November 2025

Änderungen	Beschreibung	Date
Ergänzung und Aktualisierung des Onboarding-Leitfadens	Erstellt und aktualisiert Der Onboarding-Leitfaden wurde hinzugefügt, der die folgenden Abschnitte enthält Der Abschnitt „Reaktion auf Sicherheitsvorfälle aktivieren“ wurde hinzugefügt. Der Abschnitt „Techniker für die Reaktion auf Sicherheitsvorfälle autorisieren, um Maßnahmen zur Eindämmung von Bedrohungen durchzuführen“ wurde hinzugefügt. Der Abschnitt „Reaktion auf Sicherheitsvorfälle nach der Bereitstellung“ wurde hinzugefügt. Der Abschnitt Update the Incident Response Team wurde hinzugefügt. Der Abschnitt „GuardDuty Ergebnisse und Regeln zur Unterdrückung“ wurde hinzugefügt. EventBridgeAmazon-Bereich hinzugefügt. Abschnitt Integrationen und Workflow für externe Tools hinzugefügt.	12. November 2025

Änderungen	Beschreibung	Date
	Der Abschnitt „Workflow für externe Werkzeuge“ wurde hinzugefügt. Der Abschnitt Anhang A: Ansprechpartner wurde hinzugefügt.	
Aktualisierungen zur Einhaltung von Vorschriften und zur Rechnungsstellung	Die Aussage, dass die Reaktion auf AWS Sicherheitsvorfälle in keinem Framework abgedeckt ist, wurde aktualisiert. AWS Die Reaktion auf Sicherheitsvorfälle ist jetzt im Rahmen von HITRUST abgedeckt, und in future werden weitere folgen. Sichtbarkeit und Kontrolle wurden aktualisiert, um die Reaktion auf Sicherheitsvorfälle zu erweitern AWS Die Aktualisierung „Mitgliedschaft kündigen“ wurde aktualisiert, um die Abrechnungszeiträume für Dienste zu klären Zu Getting Started wurde ein Video hinzugefügt, das zusätzlichen Kontext für typische Aufgaben bietet, um mit der Nutzung von AWS Security Incident Response zu beginnen.	15. August 2025

Änderungen	Beschreibung	Date
Aktualisiert — AWSSecurityIncidentResponseServiceRolePolicy	Die Richtlinie umfasst nun zwei neue Aktionen `"organizations:ListDelegatedAdministrators"` und eine neue Bedingung: `"organizations:DescribeAccount"` `"Condition": { "StringEquals": { "aws:ResourceAccount": "${aws:PrincipalAccount}" } }`	TBD

Änderungen	Beschreibung	Date
Funktionsupdate: Abonnieren bestimmter Organisationseinheiten (OUs) oder Ihrer gesamten Organisation AWS	Die Hilfebereiche auf der Benutzeroberfläche wurden aktualisiert und enthalten nun aktuelle Informationen zum Abonnieren bestimmter Organisationseinheiten (OUs) oder Ihrer gesamten AWS Organisation. Neue Seite für die Verwaltung von Mitgliedschaften mit Organisationseinheiten erstellt () OUs Seiten im Zusammenhang mit AWS Organizations wurden aktualisiert, um neuen Funktionen zur Verwaltung von Organisationseinheiten Rechnung zu tragen.	7. August 2025
Aktualisierte Service Quotas	Die Seite mit den Service Quotas wurde aktualisiert und führt Benutzer nun zum AWS allgemeinen Referenzleitfaden für Endpunkte und Kontingente zur Reaktion auf AWS Sicherheitsvorfälle	7. August 2025

Änderungen	Beschreibung	Date
Aktualisierungen des Benutzerfeedbacks	Es wurden Hyperlinks für den Service zu Fällen zur Reaktion auf AWS Sicherheitsvorfälle hinzugefügt Der Leitfaden zur Behandlung von Sicherheitsvorfällen (Computer Security Incident Handling Guide SP 800-61 r3) wurde für den technischen Sicherheitsleitfaden aktualisiert	7. August 2025
Seite für die EventBridge Amazon-Integration mit AWS Security Incident Response wird hinzugefügt.	Neuer Inhaltsabschnitt zur Beschreibung der EventBridge Integration von Amazon in AWS Security Incident Response.	26. Juni 2025

Änderungen	Beschreibung	Date
Aktualisierungen für SLR, mit denen Berechtigungen zur Unterstützung von Servicebe rechtigungen hinzugefügt werden.	AWSSecurityInciden tResponseTriageServiceRoleP olicywurde aktualisiert und fügt nun die Berechtig ungen security-ir:GetMem bership, security-ir:, security-ir:ListMemberships, guardduty :, guarduty:UpdateCase, guardduty: und guardduty : ListFilters hinzugefügt. guardduty: wurde hinzugefü gtUpdateFilter, um die Verwaltung von DeleteFil ter Autoarchivierungsfiltern in delegierten Konten zu erleichtern. GetAdmini stratorAccount GetAdmini stratorAccount GuardDuty	02. Juni 2025
Aktualisierungen der Ressourcen.	Die b-incident-response-resources .html #playbook - Ressourcen wurden aktualisi ert https://docs.aws.a mazon.com/security-ir/latest/ userguide/appendix, um die aktiven Workshops wiederzug eben, die unseren Kunden zur Verfügung stehen.	23. Mai 2025

Änderungen	Beschreibung	Date
Der Service unterstützt die japanische Sprache.	Die unterstützten Konfigurationen wurden aktualisiert, um die japanische Sprachunterstützung in der Japan Ortszeit zu identifizieren. Englisch wird weltweit unterstützt.	13. Mai 2025
Inhaltsaktualisierungen und Kundenfeedback.	Zu https://docs.aws.amazon.com/security-ir/ latest/userguide/select a-membership -account -.html wurde ein Hinweis hinzugefügt, der auf eine zusätzliche Aufgabe bei der Verwendung eines delegierten Administratorkontos als Teil der Installation hinweist. Die Benutzererfahrung bei der Arbeit mit einem vom Service generierten Kundenvorgang und der Funktion „Erkennen und Analysieren“ wurde aktualisiert. Die Angaben zur Kontokündigung wurden aktualisiert, um mehr Klarheit darüber zu schaffen, welche Auswirkungen die Kündigung einer Mitgliedschaft auf die Abrechnung hat.	9. Mai 2025

Änderungen	Beschreibung	Date
Drei neue unterstützte Regionen werden hinzugefügt.	Drei neue Regionen wurden zu https://docs.aws.amazon.com/security-ir/ latest/ userguide/supported -configs.html hinzugefügt. Mumbai, Paris und São Paulo.	7. Mai 2025
Aktualisiert: Aktualisierungen aufgrund von Kundenkommentaren zu Dokumenten.	Rechtschreib- und Grammatikfehler auf mehreren Seiten wurden korrigiert. https://docs.aws.amazon.com/en_us/security- ir/latest/ userguide/organizations_permissions.html wurde aktualisiert, sodass security-ir als Dienstpräfix korrekt wiedergegeben wird. Der https://docs.aws.amazon.com/security-ir/ latest/ userguide/source Datei - containment.html wurde ein Hinweis zu Route53 und DNS hinzugefügt.	7. Februar 2025

Änderungen	Beschreibung	Date
Aktualisiert: Aktualisierungen aufgrund von Kundenkommentaren zu Dokumenten.	Aktualisiert https://docs.aws.amazon.com/security-ir/ latest/userguide/setup — monitoring-and-investigation-workflows HTML zur Stackset-Vorlage. Die Einträge triage.security-ir.com bis triage.security-ir.amazonaws.com wurden korrigiert Hinweis zu verfolgten Verbindungen für 2Reversible auf .html hinzugefügt. AWSSupport-ContainEC https://docs.aws.amazon.com/security-ir/ latest/userguide/contain Ein defekter Link auf https://docs.aws.amazon.com/security-ir/ latest/userguide/managing-associated-accounts.html wurde behoben. Eine Definition für ein Mitgliedskonto wurde unter https://docs.aws.amazon.com/security-ir/ latest/userguide/select - a-membership-account .html hinzugefügt. Zu https://docs.aws.amazon.com/en_us/ security-ir/latest/userguide/using - service-linked-roles .html für	20. Dezember 2024

Änderungen	Beschreibung	Date
	AWS Organizations Verwaltungskonten wurde ein Hinweis zur Klarstellung hinzugefügt.	

Änderungen	Beschreibung	Date
Aktualisiert: Aktualisierungen aufgrund von Kundenkommentaren zu Dokumenten.	Es wurden mehrere Duplikate AWS AWS im Text entfernt. Fehlerhafte Links auf https://docs.aws.amazon.com/security-ir/ latest/userguide/sir_tagging.html and https://docs.aws.amazon.com/security-ir/latest/userguide/service - name-info-in-cloudtrail .html wurden behoben. Aktualisierungen für https://docs.aws.amazon.com/security-ir/ latest/userguide/contain .html. Das > wurde aus dem ersten Absatz entfernt. AWSSupport-ContainEC2Reversible wurde durch AWSSupport-ContainEC 2Instance ersetzt. Ersetzt durch AWSSupport-ContainIAMReversible . AWSSupport-Contain IAMPrincipal AWSSupport-ContainS3Reversible durch 3Resource AWSSupport-ContainS ersetzt. Die Formatierung auf https://docs.aws.amazon.com/en_us/security- .html wurde aktualisiert ir/latest/userguide/issues Wenn Kunden aufgefordert werden, sich über ein	10. Dezember 2024

Änderungen	Beschreibung	Date
	Supportticket an die Reaktion auf Sicherheitsvorfälle zu wenden, bietet https://docs.aws.amazon.com/security-ir/ latest/userguide/understand response-teams-and-support -.html nun Optionen, die in den Support-Formularen ausgewählt werden können. CloudWatch Ereignisse wurden entfernt und durch EventBridge on https://docs.aws.amazon.com/security -ir/ latest/userguide/logging - and-events.html ersetzt. Grammatik-Updates auf https://docs.aws.amazon.com /security-ir/ latest/userguide/technique -access-containment.html. Das Veröffentlichungsdatum wurde aus https://docs.aws.amazon.com/security-ir/ latest/ userguide/security incident-response-guide -.html entfernt und durch Aktualisierungen in dieser Tabelle ersetzt.	
Aktualisiert: AWS verwaltete Richtlinien und dienstbezogene Rollen.	Aktualisierungen der verwalteten Richtlinien und dienstbezogenen Rollen.	01. Dezember 2024

Änderungen	Beschreibung	Date
Servicestart	Erste Servicedokumente für die Einführung des Dienstes auf der re:Invent 2024	01. Dezember 2024

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.