Leitfaden zur Implementierung

Automatisierte Sicherheitsreaktion auf AWS

Automatisierte Sicherheitsreaktion auf AWS: Leitfaden zur Implementierung

Table of Contents

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

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

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

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

Die kontinuierliche Weiterentwicklung der Sicherheit erfordert proaktive Maßnahmen zur Sicherung von Daten, was es für Sicherheitsteams schwierig, teuer und zeitaufwändig machen kann, zu reagieren. Mit der Automated Security Response on AWS-Lösung können Sie schnell auf Sicherheitsprobleme reagieren, indem sie vordefinierte Antworten und Abhilfemaßnahmen bereitstellt, die auf branchenüblichen Compliance-Standards und Best Practices basieren.

Automated Security Response on AWS ist eine AWS-Lösung, die mit AWS Security Hub zusammenarbeitet, um Ihre Sicherheit zu verbessern und Ihre Workloads an den Best Practices für Well-Architected Security auszurichten (0)SEC1. Diese Lösung erleichtert es Kunden von AWS Security Hub, häufig auftretende Sicherheitsprobleme zu lösen und ihren Sicherheitsstatus in AWS zu verbessern.

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

> **Note**
>
> Die Behebung ist für Notfallsituationen vorgesehen, die sofortiges Handeln erfordern. Diese Lösung nimmt Änderungen zur Behebung von Ergebnissen nur vor, wenn sie von Ihnen über die AWS Security Hub-Managementkonsole initiiert wurden oder wenn die automatische Behebung mithilfe der EventBridge Amazon-Regel für eine bestimmte Kontrolle aktiviert wurde. Um diese Änderungen rückgängig zu machen, müssen Sie die Ressourcen manuell in ihren ursprünglichen Zustand zurückversetzen.
> Beachten Sie bei der Behebung von AWS-Ressourcen, die als Teil des CloudFormation Stacks bereitgestellt werden, dass dies zu Abweichungen führen kann. Wenn möglich, korrigieren Sie die Stack-Ressourcen, indem Sie den Code, der die Stack-Ressourcen

definiert, ändern und den Stack aktualisieren. Weitere Informationen finden Sie unter Was ist Drift? im CloudFormation AWS-Benutzerhandbuch.

Automated Security Response on AWS umfasst die Playbook-Korrekturen für die Sicherheitsstandards, die als Teil der folgenden Punkte definiert wurden:

- Zentrum für Internetsicherheit (CIS) AWS Foundations Benchmark v1.2.0
- Benchmark v1.4.0 für CIS AWS-Stiftungen
- Benchmark v3.0.0 für CIS AWS-Stiftungen
- Bewährte Methoden der AWS-Grundsicherheit (FSBP) v.1.0.0
- Datensicherheitsstandard der Zahlungskartenbranche (PCI-DSS) v3.2.1
- Nationales Institut für Standards und Technologie (NIST) SP 800-53 Rev. 5

Die Lösung umfasst auch ein Security Controls (SC) -Playbook für die Funktion konsolidierter Kontrollergebnisse von AWS Security Hub. Weitere Informationen finden Sie unter Playbooks. Wir empfehlen, das SC-Playbook zusammen mit den konsolidierten Kontrollergebnissen in Security Hub zu verwenden.

In diesem Implementierungsleitfaden werden architektonische Überlegungen und Konfigurationsschritte für die Bereitstellung der Automated Security Response on AWS-Lösung in der AWS-Cloud erörtert. Es enthält Links zu CloudFormationAWS-Vorlagen, mit denen die AWS-Rechen-, Netzwerk-, Speicher- und anderen Services gestartet, konfiguriert und ausgeführt werden, die für die Bereitstellung dieser Lösung auf AWS erforderlich sind, wobei die bewährten AWS-Methoden für Sicherheit und Verfügbarkeit verwendet werden.

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

Features und Vorteile

Die automatisierte Sicherheitsreaktion auf AWS bietet die folgenden Funktionen:

Automatisches Korrigieren von Ergebnissen bei bestimmten Kontrollen

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

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

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

Lassen Sie sich über Abhilfemaßnahmen und Ergebnisse benachrichtigen

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

Verwenden Sie die Web-Benutzeroberfläche, um Abhilfemaßnahmen zu starten, anzuzeigen und zu verwalten

Sie haben die Möglichkeit, bei der Bereitstellung des Admin-Stacks die Weboberfläche der Lösung zu aktivieren. Dadurch erhalten Sie eine umfassende, benutzerfreundliche Ansicht, in der Sie Behebungen durchführen und alle von der Lösung in der Vergangenheit durchgeführten Behebungen einsehen können.

Integrieren Sie in Ticketsysteme wie Jira oder ServiceNow

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

Verwenden Sie AWSConfig Remediations in den GovCloud Partitionen und China

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

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

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

Anwendungsfälle

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

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

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

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

Konzepte und Definitionen

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

Problembehebung, Runbook zur Problembehebung

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

Runbook steuern

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

Orchestrator

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

Standard

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

Steuerung

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

konsolidierte Kontrollergebnisse, Sicherheitskontrolle, Ansicht der Sicherheitskontrollen

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

[Solution Web UI] delegierter Administrator

Im Kontext der Weboberfläche der Lösung ist ein delegierter Administrator ein Benutzer, der vom Administrator eingeladen wurde und vollen Zugriff darauf hat, Behebungen durchzuführen und den Behebungsverlauf einzusehen. Dieser Benutzer kann auch andere Benutzer des Kontobetreibers anzeigen und verwalten.

[Solution Web UI] Kontobetreiber

Im Kontext der Weboberfläche der Lösung ist ein Kontobetreiber ein Benutzer, der von einem Administrator oder einem delegierten Administrator eingeladen wird, auf die Weboberfläche der Lösung zuzugreifen. Dieser Benutzer ist mit einer Liste von AWS-Konto-IDs verknüpft, die in seiner Einladung angegeben sind. Er kann nur Behebungen ausführen und den Behebungsverlauf einsehen, soweit er sich auf Ressourcen in diesen Konten bezieht.

Eine allgemeine Referenz zu AWS-Begriffen finden Sie im AWS-Glossar.

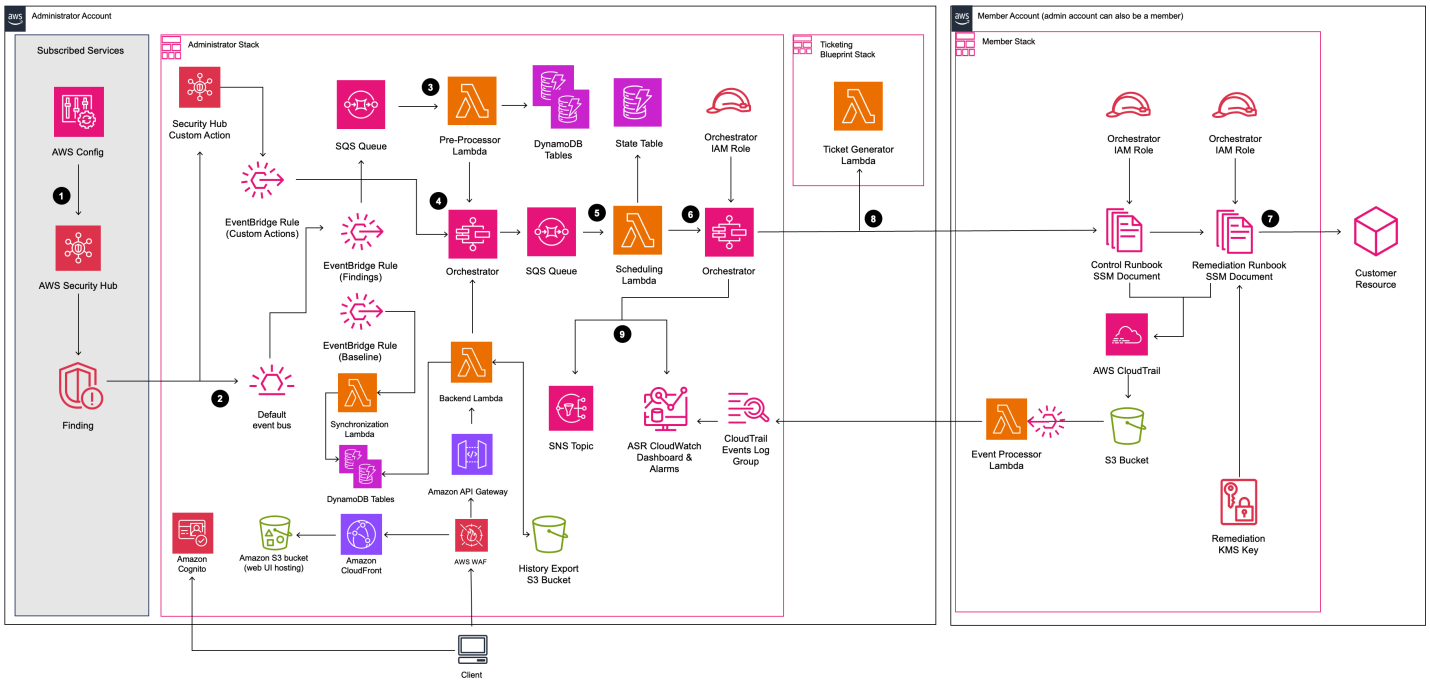
Übersicht über die Architektur

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

Architekturdiagramm

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

Automatisierte Sicherheitsreaktion auf AWS-Architektur



> **Note**
>
> CloudFormation AWS-Ressourcen werden aus Konstrukten des AWS Cloud Development Kit (AWS CDK) erstellt.

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

1. Erkennen: AWS Security Hub bietet Kunden einen umfassenden Überblick über ihren AWS-Sicherheitsstatus. Es hilft ihnen, ihre Umgebung anhand der Standards und bewährten Verfahren der Sicherheitsbranche zu messen. Es funktioniert durch das Sammeln von Ereignissen und Daten aus anderen AWS-Services wie AWS Config, Amazon Guard Duty und AWS Firewall Manager. Diese Ereignisse und Daten werden anhand von Sicherheitsstandards wie dem CIS AWS Foundations Benchmark analysiert. Ausnahmen werden als Ergebnisse in der AWS Security Hub Hub-Konsole geltend gemacht. Neue Ergebnisse werden als EventBridgeAmazon-Events gesendet.
2. Zuhören: EventBridge Ereignisse werden von AWS Security Hub für jedes Ergebnis ausgegeben, das durch den Service erstellt oder geändert wird. Automated Security Response on AWS (ASR) setzt zwei EventBridge Regeln ein, die darauf achten, dass von AWS Security Hub generierte Ereignisse gefunden werden:
   - Benutzerdefinierte EventBridge Aktionsregel: Überwacht benutzerdefinierte Aktionsereignisse, die von AWS Security Hub CSPM ausgelöst werden, wenn die benutzerdefinierte Aktion „Remediate with ASR“ von einem Benutzer ausgelöst wird. Das Ereignis wird zur Behebung an den Orchestrator weitergeleitet.
   - EventBridge Ergebnisregel: Überwacht alle Ereignisse zum Erstellen oder Aktualisieren von Ergebnissen, die von AWS Security Hub und AWS Security Hub CSPM ausgegeben werden. Diese Ereignisse werden zur weiteren Verarbeitung an die SQS-Warteschlange des Präprozessors weitergeleitet.
3. Initiieren: Sie können Behebungen manuell einleiten oder sie so konfigurieren, dass sie automatisch ausgeführt werden. Um eine Problembehebung manuell durchzuführen, können Sie die von der Lösung bereitgestellte Web-UI oder die Funktion für benutzerdefinierte Aktionen in AWS Security Hub CSPM verwenden. Nach sorgfältigen Tests in einer Umgebung außerhalb der Produktionsumgebung können Sie auch automatisierte Problembehebungen aktivieren. Sie können Automatisierungen für einzelne Behebungen aktivieren — Sie müssen die automatischen Initiierungen nicht für alle Behebungen aktivieren. Informationen zur Konfiguration der automatischen Ausführung von Behebungen finden Sie auf der Seite Vollautomatische Behebungen aktivieren.
4. Vorabbehebung: Im Administratorkonto verarbeitet AWS Step Functions das Behebungsereignis und bereitet es für die Planung vor.
5. Zeitplan: Die Lösung ruft die AWS-Lambda-Scheduling-Funktion auf, um das Behebungsereignis in der Amazon DynamoDB DynamoDB-Statustabelle zu platzieren.

6. Orchestrieren: Im Administratorkonto verwendet Step Functions kontenübergreifende AWS Identity and Access Management (IAM) -Rollen. Step Functions ruft die Problembehebung in dem Mitgliedskonto auf, das die Ressource enthält, die zu der Sicherheitslücke geführt hat.
7. Korrigieren: Ein AWS Systems Manager Automation-Dokument im Mitgliedskonto führt die zur Behebung des Fehlers auf der Zielressource erforderlichen Maßnahmen durch, z. B. die Deaktivierung des öffentlichen Lambda-Zugriffs.

   Optional können Sie die Aktionsprotokollfunktion in den Mitglieds-Stacks mit dem Log-Parameter aktivieren. EnableCloudTrailFor ASRAction Diese Funktion erfasst die von der Lösung ausgeführten Aktionen in Ihren Mitgliedskonten und zeigt sie im CloudWatchAmazon-Dashboard der Lösung an.
8. (Optional) Erstellen Sie ein Ticket: Wenn Sie den TicketGenFunctionNameParameter verwenden, um das Ticketing im Admin-Stack zu aktivieren, ruft die Lösung die bereitgestellte Lambda-Funktion für den Ticketgenerator auf. Diese Lambda-Funktion erstellt ein Ticket in Ihrem Ticketservice, nachdem die Problembehebung im Mitgliedskonto erfolgreich ausgeführt wurde. Wir bieten Stacks für die Integration mit Jira und. ServiceNow
9. Benachrichtigen und protokollieren: Das Playbook protokolliert die Ergebnisse in einer CloudWatch Protokollgruppe, sendet eine Benachrichtigung an ein Amazon Simple Notification Service (Amazon SNS) -Thema und aktualisiert den Security Hub Hub-Befund. Die Lösung führt in den Ergebnisnotizen einen Prüfpfad der Aktionen.

Überlegungen zum AWS-Well-Architected-Design

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

Operative Exzellenz

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

- Ressourcen, die als IaC definiert sind und verwenden. CloudFormation
- Soweit möglich, wurden Abhilfemaßnahmen mit den folgenden Merkmalen durchgeführt:

- Idempotenz
- Fehlerbehandlung und Berichterstattung
- Protokollierung
- Wiederherstellung eines bekannten Zustands der Ressourcen bei einem Ausfall

Sicherheit

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

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

Zuverlässigkeit

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

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

Leistungseffizienz

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

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

Kostenoptimierung

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

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

Nachhaltigkeit

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

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

Einzelheiten zur Architektur

In diesem Abschnitt werden die Komponenten und AWS-Services beschrieben, aus denen diese Lösung besteht, sowie die Architekturdetails dazu, wie diese Komponenten zusammenarbeiten.

Integration mit AWS Security Hub

Durch die Bereitstellung des `automated-security-response-admin` Stacks wird eine Integration mit der benutzerdefinierten Aktionsfunktion von AWS Security Hub CSPM erreicht. Wenn Benutzer der AWS Security Hub CSPM-Konsole auf Actions > Remediate with ASR klicken, werden die ausgewählten Ergebnisse an den Korrektur-Workflow gesendet EventBridge und lösen diesen aus.

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

Benutzer können mithilfe von Amazon DynamoDB vollautomatische Problembehebungen auf Kontrollbasis konfigurieren. Diese Option aktiviert die vollautomatische Behebung von Ergebnissen, sobald sie an AWS Security Hub gemeldet werden. Standardmäßig sind automatische Initiierungen deaktiviert. Diese Option kann jederzeit nach der Installation geändert werden, indem die DynamoDB-Tabelle für die Standardisierungskonfiguration geändert wird.

Kontoübergreifende Problembehebung

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

Spielbücher

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

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

  > **Important**
  >
  > Wenn Consolidated Control Findings in Security Hub aktiviert sind, ist dies das einzige Playbook, das in der Lösung aktiviert werden sollte.

- Center for Internet Security (CIS) Benchmarks der Amazon Web Services Foundation, Version 1.2.0, veröffentlicht am 18. Mai 2018.
- Benchmarks der Amazon Web Services Foundations des Center for Internet Security (CIS), Version 1.4.0, veröffentlicht am 9. November 2022.
- Center for Internet Security (CIS) Benchmarks der Amazon Web Services Foundation, Version 3.0.0, veröffentlicht am 13. Mai 2024.
- AWS Foundational Security Best Practices (FSBP) Version 1.0.0, veröffentlicht im März 2021.
- Version 3.2.1 der Datensicherheitsstandards der Zahlungskartenindustrie (PCI-DSS), veröffentlicht im Mai 2018.
- Version 5.0.0 des Nationalen Instituts für Standards und Technologie (NIST), veröffentlicht im November 2023.

Zentralisierte Protokollierung

Automatisierte Sicherheitsreaktionen auf AWS-Protokollen in einer einzigen CloudWatch Protokollgruppe, SO0111-ASR. Diese Protokolle enthalten eine detaillierte Protokollierung der Lösung zur Fehlerbehebung und Verwaltung der Lösung.

Benachrichtigungen

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

- SO0111-ASR_Topic — Wird verwendet, um allgemeine Informationen und Fehlermeldungen im Zusammenhang mit ausgeführten Behebungen zu senden.
- SO0111-ASR_Alarm_Topic — Wird verwendet, um zu benachrichtigen, wenn einer der Alarme der Lösung ausgelöst wird, was darauf hinweist, dass die Lösung nicht wie erwartet funktioniert.

AWS-Services in dieser Lösung

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

AWS Service	Description
Amazon EventBridge	Kern. EventBridge Regeln werden verwendet, um Ereignisse abzuhören und auszulösen, die von AWS Security Hub und AWS Security Hub CSPM ausgegeben werden.
AWS ICH	Kern. Stellt viele Rollen bereit, um Problembe hebungen auf verschiedenen Ressourcen zu ermöglichen.
AWS Lambda	Kern. Stellt mehrere Lambda-Funktionen bereit, die vom Step Function Orchestator zur Behebung von Problemen verwendet werden. Dient als Backend für die in API Gateway integrierte Weboberfläche der Lösung.
AWS Security Hub	Kern. Bietet Kunden einen umfassenden Überblick über ihren AWS-Sicherheitsstatus.

AWS Service	Description
AWS Step Functions	Kern. Stellt einen Orchestrator bereit, der die Behebungsdokumente mit API-Aufrufen von AWS Systems Manager aufruft.
AWS Systems Manager	Kern. Stellt System Manager Automation-Dokumente bereit, die die von der Lösung auszuführende Behebungslogik enthalten. Verwendet Parameter Store, um Lösungsmetadaten und Konfigurationseinstellungen zu verwalten.
AWS DynamoDB	Kern. Speichert die zuletzt ausgeführte Behebung in jedem Konto und jeder Region, um die Planung von Korrekturen zu optimieren. Speichert Ergebnisse, die von AWS Security Hub und AWS Security Hub CSPM generiert wurden. Speichert Metadaten zur Problembehebung und Lösungskonfiguration. Speichert Daten für Benutzer, die auf die Weboberfläche der Lösung zugreifen.
AWS CloudTrail	Unterstützend. Zeichnet Änderungen auf, die die Lösung an Ihren AWS-Ressourcen vornimmt, und zeigt sie auf einem CloudWatch Dashboard an.
Amazon CloudWatch	Unterstützend. Stellt Protokollgruppen bereit, die von den verschiedenen Playbooks zum Protokollieren der Ergebnisse verwendet werden. Sammelt Messwerte, die auf einem benutzerdefinierten Dashboard mit Alarmen angezeigt werden.

AWS Service	Description
Amazon Simple Notification Service	Unterstützend. Stellt SNS-Themen bereit, die eine Benachrichtigung erhalten, sobald eine Problembehebung abgeschlossen ist.
AWS SQS	Unterstützend. Hilft bei der Planung von Korrekturen, sodass die Lösung Korrekturen parallel ausführen kann. Puffert Lambda-Ausführungen mithilfe von Lambda-Mappings. EventSource
AWS Key Management Service	Unterstützend. Wird verwendet, um Daten für Problembehebungen zu verschlüsseln.
AWS Config	Unterstützend. Zeichnet alle Ressourcen zur Verwendung mit AWS Security Hub auf.
Amazon S3	Unterstützend. Speichert den exportierten Behebungsverlauf und die Protokolldaten. Hostet die Weboberfläche der Lösung als einseitige Anwendung (SPA).
Amazon CloudFront	Unterstützend. Stellt die Web-Benutzeroberfl äche der Lösung bereit
Amazon API Gateway	Unterstützend. Erstellt die REST-API der Lösung zur Unterstützung der Benutzero berfläche.
AWS WAF	Unterstützend. Schützt die Weboberfläche der Lösung.
Amazon Cognito	Unterstützend. Wird verwendet, um den Zugriff auf die Weboberfläche der Lösung zu authentif izieren und zu autorisieren.

Planen Sie Ihren Einsatz

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

Cost (Kosten)

Sie sind für die Kosten der AWS-Services verantwortlich, die für den Betrieb dieser Lösung verwendet werden.

Zum jetzigen Zeitpunkt belaufen sich die geschätzten monatlichen Kosten auf:

- Kleine Bereitstellung (10 Konten, 1 Region — USA) East/N. Virginia): Approximately $20.73 for 300 remediations/month
- Mittlere Bereitstellung (100 Konten, 1 Region — USA) East/N. Virginia): Approximately $136.57 for 3,000 remediations/month
- Umfangreicher Einsatz (1.000 Konten, 10 Regionen): Ungefähr 10.460,80 USD für 30.000 Behebungen pro Monat

> **Important**
>
> Die Preise sind freibleibend. Vollständige Informationen finden Sie auf der Preisseite für jeden AWS-Service, der in dieser Lösung verwendet wird.

> **Note**
>
> Viele AWS-Services beinhalten ein kostenloses Kontingent. Dabei handelt es sich um einen Basisbetrag des Services, den Kunden kostenlos nutzen können. Die tatsächlichen Kosten können über oder unter den angegebenen Preisbeispielen liegen.

Wir empfehlen, über den AWS Cost Explorer ein Budget zu erstellen, um die Kosten besser verwalten zu können. Die Preise sind freibleibend. Vollständige Informationen finden Sie auf der Preisseite für jeden AWS-Service, der in dieser Lösung verwendet wird.

Beispiel für eine Kostentabelle

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

- Die Anzahl der AWS Security Hub Hub-Mitgliedskonten
- Die Anzahl der aktiven, automatisch aufgerufenen Abhilfemaßnahmen
- Die Häufigkeit der Problembehebung

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

Service	Kostenloses Kontingent	Preisgestaltung [USD]
AWS Systems Manager Automation — Anzahl der Schritte	Kein kostenloses Kontingent	Jeder Basisschritt wird mit 0,002$ pro Schritt berechnet . Bei Automatisierungen mit mehreren Konten werden alle Schritte, einschließlich der Schritte, die in beliebige n Kinderkonten ausgeführt werden, nur für das ursprüngl iche Konto gezählt.
AWS Systems Manager Automation — Dauer der Schritte	Kein kostenloses Kontingent	Jeder `aws:executeScript` Aktionsschritt wird mit 0,00003$ pro Sekunde berechnet.
AWS Systems Manager Automation — Speicher	Kein kostenloses Kontingent	0,046$ pro GB pro Monat
AWS Systems Manager Automation — Datenüber tragung	Kein kostenloses Kontingent	0,900$ pro übertragenem GB (für kontoübergreifendes Konto oder) out-of-Region
AWS Security Hub CSPM — Sicherheitsüberprüfungen	Kein kostenloses Kontingent	Die ersten 100.000 checks/ac count/Region/month kosten 0,0010 USD pro Scheck

Service	Kostenloses Kontingent	Preisgestaltung [USD]
		Die nächsten 400.000 checks/account/Region/month kosten 0,0008$ pro Scheck Über 500.000 checks/account/Region/month kosten 0,0005$ pro Scheck
AWS Security Hub CSPM — Erfassungsereignisse finden	Die ersten 10.000 sind kostenlos. events/account/Region/month Suche nach Datenaufnahmeereignissen im Zusammenhang mit den Sicherheitsüberprüfungen von Security Hub.	Über 10.000$ events/account/Region/month kosten 0,00003$ pro Ereignis
Amazon CloudWatch — Metriken	Grundlegende Monitoring-Metriken (im Abstand von 5 Minuten) 10 Detaillierte Überwachungsmetriken (im Intervall von 1 Minute) 1 1 Million API-Anfragen (gilt nicht für GetMetricData, GetInsightRuleReport und GetMetricWidgetImage)	Die ersten 10.000 Metriken kosten 0,30$ pro Metrik pro Monat Die nächsten 240.000 Metriken kosten 0,10$ pro Metrik pro Monat Die nächsten 750.000 Metriken kosten 0,05$ pro Metrik pro Monat Über 1.000.000 Metriken kosten 0,02$ pro Metrik pro Monat API-Aufrufe kosten 0,01$ pro 1.000 Anfragen
Amazon CloudWatch — Armaturenbrett	3 Dashboards für bis zu 50 Metriken pro Monat	3,00$ pro Dashboard und Monat

Service	Kostenloses Kontingent	Preisgestaltung [USD]
Amazon CloudWatch — Alarme	10 Alarmmetriken (gilt nicht für hochauflösende Alarme)	Die Standardauflösung (60 Sekunden) kostet 0,10$ pro Alarmmetrik Hohe Auflösung (10 Sekunden) kostet 0,30$ pro Alarmmetrik Die Erkennung von Anomalien mit Standardauflösung kostet 0,30 USD pro Alarm Die Erkennung von Anomalien mit hoher Auflösung kostet 0,90 USD pro Alarm Composite kostet 0,50$ pro Alarm
Amazon CloudWatch — Erfassung von Protokollen	5 GB Daten (Aufnahme, Archivierung und Daten, die durch Logs Insights-Abfragen gescannt wurden)	0,50$ pro GB
Amazon CloudWatch — Speicherung von Protokollen	5 GB Daten (Aufnahme, Archivierung und Daten, die durch Logs Insights-Abfragen gescannt wurden)	0,005 USD pro GB gescannte r Daten
AWS Lambda — Anfragen	1 Mio. kostenlose Anfragen pro Monat	0,20$ pro 1 Million Anfragen

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

Service	Kostenloses Kontingent	Preisgestaltung [USD]
Amazon-DynamoDB	Die ersten 25 GB Speicherplatz sind kostenlos	Danach 2,00$ pro 1 Million konsistenter Lese- und Schreibvorgänge
AWS Key Management Service	20.000 Anfragen/Monat	1,00$ pro 1 KMS-Schlüssel. Bei KMS-Schlüsseln, die Sie automatisch oder bei Bedarf rotieren, fallen durch die erste und zweite Rotation des Schlüssels die Kosten in Höhe von 1 USD pro Monat (anteilig pro Stunde) an.
Amazon Cognito	Im Tarif Essentials sind die ersten 10.000 aktiven Nutzer pro Monat kostenlos. Hinweis: Dieses kostenlose Kontingent umfasst 50 aktive Benutzer pro Monat, wenn sich Benutzer über einen externen IdP (SAML/OIDC) authentifizieren.	0,015$ pro monatlich aktivem Benutzer bei mehr als 10.000 Benutzern.
Amazon CloudFront	Das kostenlose Kontingent umfasst 1 TB ausgehende Datenübertragung und 10.000.000 HTTP- oder HTTPS-Anfragen pro Monat.	(US/Canada/Mexico) Die ersten 9 TB kosten 0,085 USD pro Monat. Die nächsten 40 TB kosten 0,080 USD pro Monat. 0,0075$ pro HTTP-Anfrage. 0,0100$ pro HTTPS-Anfrage.

Service	Kostenloses Kontingent	Preisgestaltung [USD]
Amazon S3	Kein kostenloses Kontingent	Die ersten 50 TB kosten 0,023 USD pro GB und Monat. 0,005 USD pro 1.000 PUT-, COPY-, POST- und LIST-Anfragen. 0,0004 USD pro 1.000 GET-, SELECT- und alle anderen Anfragen.
Amazon API Gateway	1 Million REST-API-Aufrufe in den ersten 12 Monaten der Nutzung.	3,50$ pro Million für die ersten 333 Millionen API-Aufrufe.

Preisbeispiele (monatlich)

Beispiel 1:300 Problembehebungen pro Monat

- 10 Konten, 1 Region
- 30 Abhilfemaßnahmen pro account/Region/month
- 500 Security Hub Hub-Ergebnisse wurden verarbeitet pro account/Region/month
- Web-UI ist deaktiviert
- Das Aktionsprotokoll ist deaktiviert
- Gesamtkosten 20,73$ pro Monat

Service	Annahmen	Monatliche Gebühren [USD]
AWS Systems Manager Automation	Schritte: ~4 Schritte * 300 Korrekturmaßnahmen * 0,002$ = 2,40$	2,49$

Service	Annahmen	Monatliche Gebühren [USD]
	Dauer: 10 s * 300 Behebungen * 0,00003$ = 0,09$	
AWS Security Hub	Es wurden keine kostenpflichtigen Dienste genutzt	$0
CloudWatch Amazon-Protokolle	0,50$ pro GB	< 0,01$
AWS Lambda — Anfragen	300 Abhilfemaßnahmen * 7 Anfragen = 2.100 Anfragen 5.000 Ergebnisse * 1 Anfrage = 5.000 Anfragen 0,20$/1.000.000 Anfragen = 0,0000002$ pro Anfrage	0,00142$
AWS Lambda — Dauer	(512 MB Arbeitsspeicher) 4.000 ms * 300 Korrekturen * 0,0000000083$ = 0,00996$ 449 ms * 5.000 Ergebnisse * 0,0000000083$ = 0,0186$	0,029$
AWS Step Functions	19 Zustandsübergänge * 300 Korrekturen = 5.700 0,025$ * (5.700/1.000) Zustandsübergänge = 0,14$	0,14$
EventBridge Amazon-Regeln	Keine Gebühr für Regeln	$0

Service	Annahmen	Monatliche Gebühren [USD]
AWS Key Management Service	1 Schlüssel * 10 Konten * 1 Region * 1$ = 10$ (API-Anfragen verschlüsseln/entschlüsseln) (300 Behebungen x 2 Anfragen) + (5.000 Ergebnisse x 4 Anfragen) = 20.600 Anfragen 0,03$ pro 10.000 Anfragen ⇒ 0,03$ * (20.600/10.000) = 0,06$	10,06$
Amazon DynamoDB	2,00$ * 1.000.000 Lese- und Schreibvorgänge = 2,00$ (Tabelle mit den Ergebnissen) 15 MB * 10 Konten * 1 Region = 150 MB (Verlaufstabelle) 10 MB * 10 Konten * 1 Region = 100 MB 0,25 USD pro GB-Monat * 0,25 GB = 0,0625 USD	2,0625$
Amazon SQS	0,40$ * 1.000.000 Anfragen = 0,40$	0,40$
Amazon SNS	0,50$ * (600/1.000.000 Benachrichtigungen) = 0,0003$	0,0003$

Service	Annahmen	Monatliche Gebühren [USD]
Amazon CloudWatch — Metriken	(Erweiterte Metriken deaktiviert) 0,30$ * 7 benutzerdefinierte Metriken = 2,10$ 0,01$ * (300 API-Aufrufe für Put-Metriken/1.000) = 0,003$	2,10$
Amazon CloudWatch — Dashboards	3,00$ * 1 Dashboard = 3,00$	3,00$
Amazon CloudWatch — Alarme	(Erweiterte Metriken deaktiviert) 0,10$ * 4 Alarme = 0,40$	0,40$
Amazon CloudWatch — Röntgenspuren	300 Behebungen * 7 Anfragen = 2.100 Lambda-Aufrufe 5.000 Ergebnisse * 1 Anfrage = 5.000 Lambda-Aufrufe 0,000005$ pro Trace * 7.100 Traces = 0,0355$	0,0355$
Gesamt		20,73$

Beispiel 2:300 Korrekturen pro Monat (Web-UI aktiviert)

- 10 Konten, 1 Region
- 30 Abhilfemaßnahmen pro account/Region/month
- 5.000 verarbeitete Security Hub Hub-Ergebnisse pro account/Region/month
- Web-UI aktiviert
- Das Aktionsprotokoll ist deaktiviert
- Gesamtkosten 36,35 USD pro Monat

Service	Annahmen	Monatliche Gebühren [USD]
AWS Systems Manager Automation	Schritte: ~4 Schritte * 300 Korrekturmaßnahmen * 0,002$ = 2,40$ Dauer: 10 s * 300 Behebungen * 0,00003$ = 0,09$	2,49$
AWS Security Hub	Es wurden keine kostenpflichtigen Dienste genutzt	$0
CloudWatch Amazon-Protokolle	0,50$ pro GB	< 0,01$
AWS Lambda — Anfragen	300 Abhilfemaßnahmen * 7 Anfragen = 2.100 Anfragen 5.000 Ergebnisse * 1 Anfrage = 5.000 Anfragen 0,20$/1.000.000 Anfragen = 0,0000002$ pro Anfrage	0,00142$
AWS Lambda — Dauer	(512 MB Arbeitsspeicher) 4.000 ms * 300 Korrekturen * 0,0000000083$ = 0,00996$ 449 ms * 5.000 Ergebnisse * 0,0000000083$ = 0,0186$	0,029$
AWS Step Functions	19 Zustandsübergänge * 300 Korrekturen = 5.700 0,025$ * (5.700/1.000) Zustandsübergänge = 0,14$	0,14$
EventBridge Amazon-Regeln	Keine Gebühr für Regeln	$0

Service	Annahmen	Monatliche Gebühren [USD]
AWS Key Management Service	1 Schlüssel * 10 Konten * 1 Region * 1$ = 10$ (API-Anfragen verschlüsseln/entschlüsseln) (300 Behebungen x 2 Anfragen) + (5.000 Ergebnisse x 4 Anfragen) = 20.600 Anfragen 0,03$ pro 10.000 Anfragen ⇒ 0,03$ * (20.600/10.000) = 0,06$	10,06$
Amazon DynamoDB	2,00$ * 1.000.000 Lese- und Schreibvorgänge = 2,00$ (Tabelle mit den Ergebnissen) 15 MB * 10 Konten * 1 Region = 150 MB (Verlaufstabelle) 10 MB * 10 Konten * 1 Region = 100 MB 0,25 USD pro GB-Monat * 0,25 GB = 0,0625 USD	2,0625$
Amazon SQS	0,40$ * 1.000.000 Anfragen = 0,40$	0,40$
Amazon SNS	0,50$ * (600/1.000.000 Benachrichtigungen) = 0,0003$	0,0003$

Service	Annahmen	Monatliche Gebühren [USD]
Amazon CloudWatch — Metriken	(Erweiterte Metriken deaktiviert) 0,30$ * 7 benutzerdefinierte Metriken = 2,10$ 0,01$ * (300 API-Aufrufe für Put-Metriken/1.000) = 0,003$	2,10$
Amazon CloudWatch — Dashboards	3,00$ * 1 Dashboard = 3,00$	3,00$
Amazon CloudWatch — Alarme	(Erweiterte Metriken deaktiviert) 0,10$ * 4 Alarme = 0,40$	0,40$
Amazon CloudWatch — Röntgenspuren	300 Behebungen * 7 Anfragen = 2.100 Lambda-Aufrufe 5.000 Ergebnisse * 1 Anfrage = 5.000 Lambda-Aufrufe 0,000005$ pro Trace * 7.100 Traces = 0,0355$	0,0355$
Amazon Cognito	(Stufe „Essentials“) 500 aktive Nutzer pro Monat	$0

Service	Annahmen	Monatliche Gebühren [USD]
Amazon CloudFront	Regionaler Datentransfer zum Absender (pro GB) = 0,020 USD Ausgehende regionale Datenübertragung ins Internet (pro GB) = 0,085 USD Preisanfrage für alle HTTP-Methoden (pro 10.000) = 0,0075 USD	0,1125$
Amazon S3	(UI-Hosting) 0,023$ pro GB * 0,002 GB = 0,000046$ (Historischer Export) 0,023 USD pro GB * 0,50 GB = 0,0125 USD 0,0004 USD pro 1.000 GET-Anfragen	0,0125 USD
AWS WAF	1 Web-ACL = 5,00 USD pro Monat 7 Regeln * 1,00$ pro Regel = 7,00$	12$
Amazon API Gateway	3,50$ pro Million REST-API-Aufrufe	3,50$
Gesamt		36,35$

Beispiel 3:3.000 Problembehebungen pro Monat

- 100 Konten, 1 Region
- 30 Abhilfemaßnahmen pro account/Region/month
- 500 Security Hub Hub-Ergebnisse wurden verarbeitet pro account/Region/month
- Web-UI ist deaktiviert
- Das Aktionsprotokoll ist deaktiviert
- Gesamtkosten 136,57 USD pro Monat

Service	Annahmen	Monatliche Gebühren [USD]
AWS Systems Manager Automation	Schritte: ~4 Schritte * 3.000 Korrekturmaßnahmen * 0,002$ = 24,00$ Dauer: 10 s * 3.000 Behebungen * 0,00003$ = 0,90$	24,90$
AWS Security Hub	Es wurden keine kostenpfl ichtigen Dienste genutzt	$0
CloudWatch Amazon-Pr otokolle	0,50$ pro GB	< 0,01$
AWS Lambda — Anfragen	3.000 Abhilfemaßnahmen * 7 Anfragen = 2.100 Anfragen 50.000 Ergebnisse * 1 Anfrage = 50.000 Anfragen 0,20$/1.000.000 Anfragen = 0,0000002$ pro Anfrage	0,01$
AWS Lambda — Dauer	(512 MB Arbeitsspeicher) 4.000 ms * 3.000 Behebungen * 0,0000000083$ = 0,0996$	0,29$

Service	Annahmen	Monatliche Gebühren [USD]
	449 ms * 50.000 Ergebnisse * 0,0000000083$ = 0,186$	
AWS Step Functions	19 Zustandsübergänge * 3.000 Korrekturen = 57.000 0,025$ * (57.000/1.000) Zustandsübergänge = 1,425$	1,425$
EventBridge Amazon-Regeln	Keine Gebühr für Regeln	$0
AWS Key Management Service	1 Schlüssel * 100 Konten * 1 Region * 1$ = 100$ (API-Anfragen verschlüsseln/entschlüsseln) (3.000 Behebungen x 2 Anfragen) + (50.000 Ergebnisse x 4 Anfragen) = 206.000 Anfragen 0,03$ pro 10.000 Anfragen ⇒ 0,03$ * (206.000/10.000) = 0,618$	100,618$
Amazon DynamoDB	2,00$ * 1.000.000 Lese- und Schreibvorgänge = 2,00$ (Tabelle mit den Ergebnissen) 15 MB x 100 Konten * 1 Region = 1.500 MB (Verlaufstabelle) 10 MB * 100 Konten * 1 Region = 1.000 MB 0,25 USD pro GB-Monat * 2,5 GB = 0,625 USD	2,625$

Service	Annahmen	Monatliche Gebühren [USD]
Amazon SQS	0,40$ * 1.000.000 Anfragen = 0,40$	0,40$
Amazon SNS	0,50$ * 1.000.000 Benachrichtigungen = 0,50$	0,50$
Amazon CloudWatch — Metriken	(Erweiterte Metriken deaktiviert) 0,30$ * 7 benutzerdefinierte Metriken = 2,10$ 0,01$ * (3000/1.000) API-Aufrufe für Put-Metriken = 0,03$	2,13$
Amazon CloudWatch — Dashboards	3,00$ * 1 Dashboard = 3,00$	3,00$
Amazon CloudWatch — Alarme	0,10$ * 4 Alarme = 0,40$	0,40$
Amazon CloudWatch — Röntgenspuren	3.000 Behebungen * 7 Anfragen = 2.100 Lambda-Aufrufe 50.000 Ergebnisse * 1 Anfrage = 50.000 Lambda-Aufrufe 0,000005$ pro Trace * 52.100 Traces = 0,2605$	0,2605$
Gesamt		136,57$

Beispiel 4:30.000 Problembehebungen pro Monat

- 1.000 Konten, 10 Regionen

- 30 Abhilfemaßnahmen pro account/Region/month
- 500 Security Hub Hub-Ergebnisse wurden verarbeitet pro account/Region/month
- Web-UI ist deaktiviert
- Das Aktionsprotokoll ist deaktiviert
- Gesamtkosten 10.460,80 USD pro Monat

Service	Annahmen	Monatliche Gebühren [USD]
AWS Systems Manager Automation	Schritte: ~4 Schritte * 30.000 Korrekturmaßnahmen * 0,002$ = 240,00$ Dauer: 10 s * 30.000 Behebungen * 0,00003$ = 9,00$	249,00$
AWS Security Hub	Es wurden keine kostenpflichtigen Dienste genutzt	$0
CloudWatch Amazon-Protokolle	0,50$ pro GB	< 0,01$
AWS Lambda — Anfragen	30.000 Behebungen * 7 Anfragen = 210.000 Anfragen 5.000.000 Ergebnisse * 1 Anfrage = 5.000.000 Anfragen 0,20$/1.000.000 Anfragen = 0,0000002$ pro Anfrage	1,042$
AWS Lambda — Dauer	(512 MB Arbeitsspeicher) 4.000 ms * 30.000 Behebungen * 0,0000000083$ = 0,996$ 449 ms * 5.000.000 Ergebnisse * 0,0000000083$ = 18,63$	19,63$

Service	Annahmen	Monatliche Gebühren [USD]
AWS Step Functions	19 Zustandsübergänge * 30.000 Korrekturen = 570.000 0,025$ * (570.000/1.000) Zustandsübergänge = 14,25$	14,25$
EventBridge Amazon-Regeln	Keine Gebühr für Regeln	$0
AWS Key Management Service	(1 Schlüssel) 1$ * 1.000 Konten * 10 Region = 10.000$ (API-Anfragen verschlüsseln/entschlüsseln) (30.000 Behebungen x 2 Anfragen) + (5.000.000 Ergebnisse x 4 Anfragen) = 20.060.000 Anfragen 0,03$ pro 10.000 Anfragen ⇒ 0,03$ * (20.06.000/10.000) = 60,18$	10.060,18$
Amazon DynamoDB	2,00$ * (10.000.000 Lese- und Schreibvorgänge/1.000.000) = 20,00$ (Tabelle mit den Ergebnissen) 15 MB x 1000 Konten * 10 Regionen = 150 GB (Verlaufstabelle) 10 MB * 1000 Konten * 10 Region = 100 GB 0,25 USD pro GB-Monat * 250 GB = 62,50 USD	82,50$

Service	Annahmen	Monatliche Gebühren [USD]
Amazon SQS	0,40$ * (5.060.000 Anfragen/ 1.000.000) = 2,024$	2,024$
Amazon SNS	0,000005$ * 1.000.000 Benachrichtigungen = 0,50$	0,50$
Amazon CloudWatch — Metriken	(Erweiterte Metriken deaktiviert) 0,30$ * 7 benutzerdefinierte Metriken = 2,10$ 0,01$ * (30.000/1.000) API-Aufrufe für Put-Metriken = 0,30$	2,40$
Amazon CloudWatch — Dashboards	3,00$ * 1 Dashboard = 3,00$	3,00$
Amazon CloudWatch — Alarme	(Erweiterte Metriken deaktiviert) 0,10$ * 4 Alarme = 0,40$	0,40$
Amazon CloudWatch — Röntgenspuren	30.000 Behebungen * 7 Anfragen = 210.000 Lambda-Aufrufe 5.000.000 Ergebnisse * 1 Anfrage = 5.000.000 Lambda-Aufrufe 0,000005$ pro Trace * 5.210.000 Traces = 26,05$	26,05$
Gesamt		10.460,80$

Beispiel 5:30.000 Korrekturen pro Monat (Web-UI aktiviert)

- 1.000 Konten, 10 Regionen
- 30 Abhilfemaßnahmen pro account/Region/month
- 500 Security Hub Hub-Ergebnisse wurden verarbeitet pro account/Region/month
- Web-UI aktiviert
- Das Aktionsprotokoll ist deaktiviert
- Gesamtkosten 10.480,90 USD pro Monat

Service	Annahmen	Monatliche Gebühren [USD]
AWS Systems Manager Automation	Schritte: ~4 Schritte * 30.000 Korrekturmaßnahmen * 0,002$ = 240,00$ Dauer: 10 s * 30.000 Behebungen * 0,00003$ = 9,00$	249,00$
AWS Security Hub	Es wurden keine kostenpflichtigen Dienste genutzt	$0
CloudWatch Amazon-Protokolle	0,50$ pro GB	< 0,01$
AWS Lambda — Anfragen	30.000 Behebungen * 7 Anfragen = 210.000 Anfragen 5.000.000 Ergebnisse * 1 Anfrage = 5.000.000 Anfragen 0,20$/1.000.000 Anfragen = 0,0000002$ pro Anfrage	1,042$
AWS Lambda — Dauer	(512 MB Arbeitsspeicher) 4.000 ms * 30.000 Behebungen * 0,0000000083$ = 0,996$	19,63$

Service	Annahmen	Monatliche Gebühren [USD]
	449 ms * 5.000.000 Ergebniss e * 0,0000000083$ = 18,63$	
AWS Step Functions	19 Zustandsübergänge * 30.000 Korrekturen = 570.000 0,025$ * (570.000/1.000) Zustandsübergänge = 14,25$	14,25$
EventBridge Amazon-Regeln	Keine Gebühr für Regeln	$0
AWS Key Management Service	(1 Schlüssel) 1$ * 1.000 Konten * 10 Region = 10.000$ (API-Anfragen verschlüsseln/ entschlüsseln) (30.000 Behebungen x 2 Anfragen) + (5.000.000 Ergebnisse x 4 Anfragen) = 20.060.000 Anfragen 0,03$ pro 10.000 Anfragen ⇒ 0,03$ * (20.06.000/10.000) = 60,18$	10.060,18$

Service	Annahmen	Monatliche Gebühren [USD]
Amazon DynamoDB	2,00$ * (10.000.000 Lese- und Schreibvorgänge/1.000.000) = 20,00$ (Tabelle mit den Ergebnissen) 15 MB x 1000 Konten * 10 Regionen = 150 GB (Verlaufstabelle) 10 MB * 1000 Konten * 10 Region = 100 GB 0,25 USD pro GB-Monat * 250 GB = 62,50 USD	82,50$
Amazon SQS	0,40$ * (5.060.000 Anfragen/1.000.000) = 2,024$	2,024$
Amazon SNS	0,000005$ * 1.000.000 Benachrichtigungen = 0,50$	0,50$
Amazon CloudWatch — Metriken	(Erweiterte Metriken deaktiviert) 0,30$ * 7 benutzerdefinierte Metriken = 2,10$ 0,01$ * (30.000/1.000) API-Aufrufe für Put-Metriken = 0,30$	2,40$
Amazon CloudWatch — Dashboards	3,00$ * 1 Dashboard = 3,00$	3,00$
Amazon CloudWatch — Alarme	(Erweiterte Metriken deaktiviert) 0,10$ * 4 Alarme = 0,40$	0,40$

Service	Annahmen	Monatliche Gebühren [USD]
Amazon CloudWatch — Röntgenspuren	30.000 Behebungen * 7 Anfragen = 210.000 Lambda-Aufrufe 5.000.000 Ergebnisse * 1 Anfrage = 5.000.000 Lambda-Aufrufe 0,000005$ pro Trace * 5.210.000 Traces = 26,05$	26,05$
Amazon Cognito	(Stufe „Essentials“) 5.000 aktive Nutzer pro Monat	$0
Amazon CloudFront	Regionaler Datentransfer zum Absender (pro GB) = 0,020 USD Ausgehende regionale Datenübertragung ins Internet (pro GB) = 0,085 USD Preisanfrage für alle HTTP-Methoden (pro 10.000) = 0,0075 USD	0,1125$

Service	Annahmen	Monatliche Gebühren [USD]
Amazon S3	(UI-Hosting) 0,023$ pro GB * 0,002 GB = 0,000046$ (Historischer Export) 0,023 USD pro GB x 100 GB = 2,30 USD 0,0004 USD pro 1.000 GET-Anfragen * 5.000 Anfragen = 2,00 USD	4,30$
AWS WAF	1 Web-ACL = 5,00 USD pro Monat 7 Regeln * 1,00$ pro Regel = 7,00$	12$
Amazon API Gateway	3,50$ pro Million REST-API-Aufrufe	3,50$
Gesamt		10.480,90$

Important

Kosten für die KMS-Schlüsselrotation Der AWS Key Management Service (KMS) rotiert die vom Kunden verwalteten Schlüssel automatisch einmal pro Jahr, wenn die Rotation aktiviert ist. Für jede Rotation fallen Kosten in Höhe von 1,00 USD pro Schlüssel und Jahr an. Bei 1000 Konten in einer einzigen Region führt dies beispielsweise zu zusätzlichen 1000 USD/Jahr (1 Umdrehung × 1000 Schlüssel × 1,00 USD).

Zusätzliche Kosten für optionale Funktionen

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

Verbesserte CloudWatch Metriken

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

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

CloudTrail Aktionsprotokoll

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

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

Service	Annahmen	Monatliche Gebühren [USD]
AWS CloudTrail	150.000 * 2,00 USD/100.000 = 3,00 USD	3,00$
Lambda	150.000 * 0,2 * 0,125 = 3.750 GB-Sekunden 3.750 * 0,0000166667$ = 0,0625$ Rechenzeit 0,15 * 0,20$ = 0,03$ Anforderungskosten 0,0625$ + 0,03$ = 0,0952$ Gesamtkosten für Lambda	0,0925$
Gesamt		3,09$ pro Mitgliedskonto

Sicherheit

Wenn Sie Systeme auf der AWS-Infrastruktur aufbauen, werden Sie und AWS gemeinsam für die Sicherheit verantwortlich sein. Dieses gemeinsame Modell reduziert Ihren betrieblichen Aufwand, da AWS die Komponenten wie das Host-Betriebssystem, die Virtualisierungsebene und die physische Sicherheit der Einrichtungen, in denen die Services betrieben werden, betreibt, verwaltet und kontrolliert. Weitere Informationen zur AWS-Sicherheit finden Sie unter AWS Cloud Security.

Sicherheitsrichtlinie für API Gateway

Wenn Sie sich dafür entscheiden, die Web-Benutzeroberfläche der Lösung zu aktivieren, wird neben dem CloudFormation Admin-Stack, der als Backend für alle Operationen in der Web-UI dient, eine API-Gateway-REST-API bereitgestellt. Die von der Lösung bereitgestellte REST-API verwendet die standardmäßige TLS-Sicherheitsrichtlinie für API Gateway, die `TLS-1-0` für die Region gilt APIs.

Nach der Bereitstellung des CloudFormation Admin-Stacks können Sie jedoch die REST-API der Lösung anpassen, indem Sie eine restriktivere TLS-Sicherheitsrichtlinie hinzufügen. Sie können beispielsweise festlegen, `TLS_1_2 security policy` dass der Datenverkehr mit TLSv1 .2 oder

TLSv1 .3 eingeschränkt werden soll. Sie finden die REST-API der Lösung in der API Gateway Gateway-Konsole unter dem Namen AutomatedSecurityResponseApi.

Um eine Sicherheitsrichtlinie für die REST-API der Lösung auszuwählen, müssen Sie zunächst einen benutzerdefinierten Domainnamen konfigurieren. Weitere Informationen finden Sie unter Benutzerdefinierter Domainname für öffentliche REST APIs in API Gateway.

Weitere Informationen zum Hinzufügen einer Sicherheitsrichtlinie zu Ihrer REST-API finden Sie unter Wählen Sie eine Sicherheitsrichtlinie für Ihre benutzerdefinierte REST-API-Domain in API Gateway im API Gateway Gateway-Handbuch.

IAM-Rollen

AWS Identity and Access Management (IAM) -Rollen ermöglichen es Kunden, Services und Benutzern in der AWS-Cloud detaillierte Zugriffsrichtlinien und -berechtigungen zuzuweisen. Diese Lösung erstellt IAM-Rollen, die den automatisierten Funktionen der Lösung Zugriff gewähren, um Korrekturmaßnahmen innerhalb eines engen Umfangs von Berechtigungen durchzuführen, die für jede Korrektur spezifisch sind.

Die Step-Funktion des Administratorkontos ist der Rolle SO0111- zugewiesen. ASR-Orchestrator-Admin Nur diese Rolle darf das SO0111-Orchestrator-Mitglied in jedem Mitgliedskonto übernehmen. Die Mitgliedsrolle darf von jeder Behebungsrolle an den AWS Systems Manager Manager-Service übergeben werden, um bestimmte Behebungs-Runbooks auszuführen.
Die Namen der Behebungsrollen beginnen mit SO0111, gefolgt von einer Beschreibung, die dem Namen des Behebungs-Runbooks entspricht. Beispielsweise ist SO0111-Remove VPCDefault SecurityGroupRules die Rolle für das ASR-Remove-Wartungs-Runbook. VPCDefault SecurityGroupRules

Unterstützte AWS Regionen

> **Important**
>
> Durch die Aktivierung optionaler Funktionen in der Lösung kann die Liste der Regionen, die für die Bereitstellung unterstützt werden, reduziert werden. Mit anderen Worten, die folgende Liste bezieht sich nur auf die Kernkomponenten der Lösung. Wenn Sie sich beispielsweise dafür entscheiden, die Webbenutzeroberfläche zu aktivieren, können Sie die Lösung nicht in GovCloud Regionen bereitstellen, da CloudFront sie in GovCloud (USA) ab November 2025 nicht unterstützt wird.

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

Name der Region	Regionscode
Europa (Paris)	eu-west-3
Europa (Spanien)	eu-south-2
Europa (Stockholm)	eu-north-1
Europa (Zürich)	eu-central-2
Naher Osten (Bahrain)	me-south-1
Naher Osten (VAE)	me-central-1
Südamerika (São Paulo)	sa-east-1
AWS GovCloud (USA-Ost)	us-gov-east-1
AWS GovCloud (USA West)	us-gov-west-1
China (Beijing)	cn-north-1
China (Ningxia)	cn-northwest-1
Israel (Tel Aviv)	il-central-1
Kanada West (Calgary)	ca-west-1
Mexiko (Mexiko)	mx-central-1
Asien-Pazifik (Thailand)	ap-southeast-7
Asien-Pazifik (Malaysia)	ap-southeast-5

Note

Alle neuen AWS-Regionen, die nicht aufgeführt sind, werden möglicherweise über eine lokale Bereitstellung unterstützt, jedoch nicht über eine Bereitstellung mit einem Klick.

Kontingente

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

Kontingente für AWS-Services in dieser Lösung

Stellen Sie sicher, dass Sie über ein ausreichendes Kontingent für jeden der in dieser Lösung implementierten Services verfügen. Weitere Informationen finden Sie unter AWS-Servicekontingente.

Verwenden Sie die folgenden Links, um zur Seite für diesen Service zu gelangen. Um die Service Quotas für alle AWS-Services in der Dokumentation anzuzeigen, ohne zwischen den Seiten zu wechseln, sehen Sie sich stattdessen die Informationen auf der Seite Service-Endpunkte und Kontingente in der PDF-Datei an.

CloudFormation AWS-Kontingente

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

CloudWatch AWS-Kontingente

Ihr AWS-Konto hat CloudWatch AWS-Kontingente, die an CloudWatch Ressourcenrichtlinien gebunden sind, sodass nur 10 Ressourcenrichtlinien pro Region und Konto zulässig sind. Diese können nicht für eine Kontingenterhöhung beantragt werden. Weitere Informationen finden Sie unter CloudWatch AWS-Logs-Kontingente im CloudWatch AWS-Benutzerhandbuch. Bitte überprüfen Sie vor Ihrer Bereitstellung Ihre aktuelle Nutzung, um sicherzustellen, dass Sie diesen Schwellenwert bei der Bereitstellung der Lösung nicht überschreiten.

AWS Organizations

Die Lambda-Funktionen der Lösung rufen die AWS Organizations API auf, um den Alias des aktuellen Kontos abzurufen und in Nachrichten aufzunehmen, die unter dem SNS-Thema der Lösung veröffentlicht wurden. Auf diese Weise können von Menschen lesbare Kontonamen in den Benachrichtigungen der Lösung zu Debugging- und Tracking-Zwecken angezeigt werden.

AWS Organizations begrenzt, wie oft Kunden ihre API-Endpunkte aufrufen können. Wenn Sie feststellen, dass die Lösung die für Ihr Konto festgelegten Grenzwerte überschreitet, können Sie die Funktion deaktivieren, mit der der Kontoalias abgerufen und angezeigt wird.

Navigieren Sie dazu zu der Lambda-Funktion mit dem Namen, die `SO0111-ASR-sendNotifications` sich in der Region und dem Konto befindet, in denen Sie den Admin-Stack bereitgestellt haben. Suchen Sie dann die angegebene Umgebungsvariable `DISABLE_ACCOUNT_ALIAS_LOOKUP` und ändern Sie den Wert von „False“ in „True“. Das Kontoaliasfeld in den Benachrichtigungen der Lösung lautet jetzt „Unbekannt“, was sich jedoch nicht auf die Funktionalität der Lösung auswirkt.

Bereitstellung von AWS Security Hub

Die Bereitstellung und Konfiguration von AWS Security Hub ist eine Voraussetzung für diese Lösung. Weitere Informationen zur Einrichtung von AWS Security Hub CSPM finden Sie unter Setting up AWS Security Hub CSPM im AWS Security Hub Hub-Benutzerhandbuch. Diese Lösung unterstützt auch AWS Security Hub (Nicht-CSPM-Version). Weitere Informationen zur Einrichtung von AWS Security Hub finden Sie unter Enabling Security Hub.

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

Stack im Vergleich zur Bereitstellung StackSets

Mit einem Stack-Set können Sie Stacks in AWS-Konten in AWS-Regionen mithilfe einer einzigen CloudFormation AWS-Vorlage erstellen. Ab Version 1.4 unterstützt diese Lösung die Bereitstellung von Stack-Sets, indem Ressourcen je nachdem, wo und wie sie bereitgestellt werden, aufgeteilt werden. Kunden mit mehreren Konten, insbesondere solche, die AWS Organizations verwenden, können von der Verwendung von Stack-Sets für die Bereitstellung auf vielen Konten profitieren. Dies reduziert den Aufwand für die Installation und Wartung der Lösung. Weitere Informationen StackSets dazu finden Sie unter Using AWS CloudFormation StackSets.

Stellen Sie die Lösung bereit

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

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

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

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

Entscheiden, wo jeder Stack eingesetzt werden soll

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

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

Der Admin-Stack muss einmal in einem einzigen Konto und in einer einzigen Region bereitgestellt werden. Es muss in dem Konto und der Region bereitgestellt werden, die Sie als Aggregationsziel

für Security Hub Hub-Ergebnisse für Ihre Organisation konfiguriert haben. Wenn Sie die Action Log-Funktion zur Überwachung von Verwaltungsereignissen verwenden möchten, müssen Sie den Admin-Stack im Verwaltungskonto Ihrer Organisation oder in einem delegierten Administratorkonto bereitstellen.

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

> **Important**
>
> Wenn Sie AWS Security Hub (nicht CSPM) verwenden, sind Sie dafür verantwortlich, dass Ihre Mitgliedskonten, die bei AWS Security Hub CSPM angemeldet sind, auch bei AWS Security Hub (nicht CSPM) integriert sind. In AWS Security Hub CSPM aggregierte Regionen sollten auch mit Regionen übereinstimmen, die in AWS Security Hub aggregiert wurden (nicht CSPM).

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

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

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

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

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

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

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

Entscheiden Sie, wie die einzelnen Stacks bereitgestellt werden

Die Optionen für die Bereitstellung eines Stacks sind

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

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

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

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

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

Konsolidierte Kontrollergebnisse

Die Konten in Ihrer Organisation können so konfiguriert werden, dass die Funktion für konsolidierte Kontrollergebnisse von Security Hub aktiviert oder deaktiviert wird. Weitere Informationen finden Sie im AWS Security Hub Hub-Benutzerhandbuch unter Ergebnisse konsolidierter Kontrollen.

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

Einsatz in China

Die Lösung unterstützt die Bereitstellung in China Regionen, Sie müssen jedoch die folgenden Startschaltflächen für die Bereitstellung mit einem Klick verwenden und nicht die Startschaltflächen in anderen Abschnitten dieses Handbuchs. Die Verwendung der Schaltflächen „Lösung starten“ in den nächsten Abschnitten dieses Handbuchs funktioniert nicht, wenn Sie in China Regionen bereitstellen. Sie können die Vorlagen weiterhin von einem beliebigen S3-Bucket-Link herunterladen und die Stacks bereitstellen, indem Sie die Vorlagendatei hochladen.

- automated-security-response-admin.vorlage:

Launch solution

- automated-security-response-member-rollen.vorlage:

- automated-security-response-member.vorlage:

GovCloud Einsatz (in den USA)

Die Lösung unterstützt zwar die Bereitstellung in Regionen GovCloud (USA), Sie müssen jedoch die folgenden Startschaltflächen für die Bereitstellung mit einem Klick verwenden und nicht die Startschaltflächen in anderen Abschnitten dieses Handbuchs. GovCloud Die Verwendung der Schaltflächen „Lösung starten“ in den nächsten Abschnitten dieses Handbuchs funktioniert nicht, wenn Sie die Bereitstellung in Regionen GovCloud (USA) durchführen. Sie können die Vorlagen weiterhin von einem beliebigen S3-Bucket-Link herunterladen und die Stacks bereitstellen, indem Sie die Vorlagendatei hochladen.

- automated-security-response-admin.vorlage:

- automated-security-response-member-rollen.vorlage:

- automated-security-response-member.vorlage:

CloudFormation AWS-Vorlagen

automa

security-response-admin.template — Verwenden Sie diese Vorlage, um die Automated Security Response on AWS-Lösung zu starten. Die Vorlage installiert die Kernkomponenten der Lösung, einen verschachtelten Stack für die AWS Step Functions Functions-Protokolle und einen verschachtelten Stack für jeden Sicherheitsstandard, den Sie aktivieren möchten.

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

Unterstützung für Administratorkonten

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

automated-security-response-orchestrator-log.template — Erstellt eine CloudWatch Protokollgruppe für die Orchestrator-Step-Funktion.

automated-security-response-webui-nested-stack.template — Erstellt die Ressourcen zur Unterstützung der Weboberfläche der Lösung.

AFSBPStack.template — Regeln für bewährte Methoden der AWS Foundational Security v1.0.0.

CIS120stack.Template — CIS Amazon Web Services Foundations Benchmarks, v1.2.0-Regeln.

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

CIS300Stack.Template — CIS Amazon Web Services Foundations Benchmarks, v3.0.0-Regeln.

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

NISTStack.template — Regeln des Nationalen Instituts für Standards und Technologie (NIST), Version 5.0.0.

SCStack.template — Regeln für Security Controls v2.0.0.

Rollen der Mitglieder

View template

automa

security-response-member-roles.template — Definiert die Wiederherstellungsrollen, die in jedem AWS Security Hub-Mitgliedskonto benötigt werden.

Mitgliedskonten

View template

automa

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

Die `automated-security-response-member.template` installiert die folgenden Vorlagen auf der Grundlage Ihrer Auswahl:

automated-security-response-remediation-runbooks.template — Allgemeiner Problembehebungscode, der von einem oder mehreren Sicherheitsstandards verwendet wird.

AFSBPMemberStack.template — AWS Foundational Security Best Practices v1.0.0 Runbooks für Einstellungen, Berechtigungen und Problembehebungen.

CIS120 MemberStack .template — Benchmarks der CIS Amazon Web Services Foundations, Version 1.2.0, Einstellungen, Berechtigungen und Runbooks zur Problembehebung.

CIS140 MemberStack .template — Benchmarks der CIS Amazon Web Services Foundations, Version 1.4.0, Einstellungen, Berechtigungen und Runbooks zur Problembehebung.

CIS300 MemberStack .template — Benchmarks der CIS Amazon Web Services Foundations, Version 3.0.0, Einstellungen, Berechtigungen und Runbooks zur Problembehebung.

PCI321MemberStack.template — PCI-DSS v3.2.1-Runbooks für Einstellungen, Berechtigungen und Problembehebungen.

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

SCMemberStack.template — Runbooks für Einstellungen, Berechtigungen und Problembehebungen von Security Control.

automated-security-response-member-cloudtrail.template — Wird in der Aktionsprotokollfunktion zur Nachverfolgung und Prüfung von Serviceaktivitäten verwendet.

Integration des Ticketsystems

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

View template

JiraBlu

— Bereitstellen, wenn Sie Jira als Ticketsystem verwenden.

View template

Service

— Bereitstellen, wenn Sie es ServiceNow als Ticketsystem verwenden.

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

Automatisierte Bereitstellung - StackSets

> **Note**
>
> Wir empfehlen die Bereitstellung mit. StackSets Für Bereitstellungen mit einem einzigen Konto oder zu Test- oder Evaluierungszwecken sollten Sie jedoch die Bereitstellungsoption Stacks in Betracht ziehen.

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

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

Voraussetzungen

AWS Organizations hilft Ihnen dabei, Ihre AWS-Umgebung und Ressourcen mit mehreren Konten zentral zu verwalten und zu steuern. StackSets funktioniert am besten mit AWS Organizations.

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

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

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

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

Bitte beachten Sie, dass diese Lösung sowohl mit AWS Security Hub als auch mit AWS Security Hub CSPM funktioniert.

Überblick über die Bereitstellung

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

Stellen Sie das StackSets von einem delegierten Administratorkonto in Ihren AWS Organizations aus bereit.

Planung

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

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

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

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

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

- Starten Sie die `automated-security-response-admin.template` CloudFormation AWS-Vorlage mithilfe einer selbstverwalteten StackSet Version in Ihrem AWS Security Hub-Administratorkonto in derselben Region wie Ihr Security Hub-Administrator. Diese Vorlage verwendet verschachtelte Stacks.
- Wählen Sie aus, welche Sicherheitsstandards installiert werden sollen. Standardmäßig ist nur SC ausgewählt (empfohlen).
- Wählen Sie eine vorhandene Orchestrator-Protokollgruppe aus, die Sie verwenden möchten. Wählen Sie aus`Yes`, ob diese `SO0111-ASR- Orchestrator` bereits in einer früheren Installation vorhanden ist.

- Wählen Sie aus, ob die Weboberfläche der Lösung aktiviert werden soll. Wenn Sie diese Funktion aktivieren möchten, müssen Sie auch eine E-Mail-Adresse eingeben, um eine Administratorrolle zu erhalten.
- Wählen Sie Ihre Einstellungen für die Erfassung von CloudWatch Metriken aus, die sich auf den Betriebsstatus der Lösung beziehen.

Weitere Informationen zur Selbstverwaltung StackSets finden Sie unter Gewähren selbstverwalteter Berechtigungen im CloudFormation AWS-Benutzerhandbuch.

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

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

- Starten Sie die `automated-security-response-member-roles.template` CloudFormation AWS-Vorlage mithilfe eines Service-Managed StackSet in einer einzigen Region in jedem Konto in Ihren AWS Organizations.
- Wählen Sie, ob diese Vorlage automatisch installiert werden soll, wenn der Organisation ein neues Konto beitritt.
- Geben Sie die Konto-ID Ihres AWS Security Hub-Administratorkontos ein.
- Geben Sie einen Wert für ein`namespace`, der verwendet wird, um Konflikte zwischen Ressourcennamen bei einer vorherigen oder gleichzeitigen Bereitstellung in demselben Konto zu verhindern. Geben Sie eine Zeichenfolge mit bis zu 9 alphanumerischen Kleinbuchstaben ein.

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

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

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

- Wählen Sie aus, welche Security Standard-Playbooks installiert werden sollen.
- Geben Sie den Namen einer CloudTrail Protokollgruppe an (die bei einigen Problembehebungen verwendet wird).
- Geben Sie die Konto-ID Ihres AWS Security Hub-Administratorkontos ein.
- Geben Sie einen Wert für ein`namespace`, der verwendet wird, um Konflikte zwischen Ressourcennamen bei einer vorherigen oder gleichzeitigen Bereitstellung in demselben Konto zu verhindern. Geben Sie eine Zeichenfolge mit bis zu 9 alphanumerischen Kleinbuchstaben ein. Dieser Wert sollte mit dem `namespace` Wert übereinstimmen, den Sie für den Mitgliederrollen-Stack ausgewählt haben. Außerdem muss der Namespace-Wert nicht für jedes Mitgliedskonto eindeutig sein.

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

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

   So stellen Sie den Jira-Stack bereit:

   a. Geben Sie einen Namen für Ihren Stack ein.

   b. Geben Sie den URI für Ihre Jira-Instanz ein.

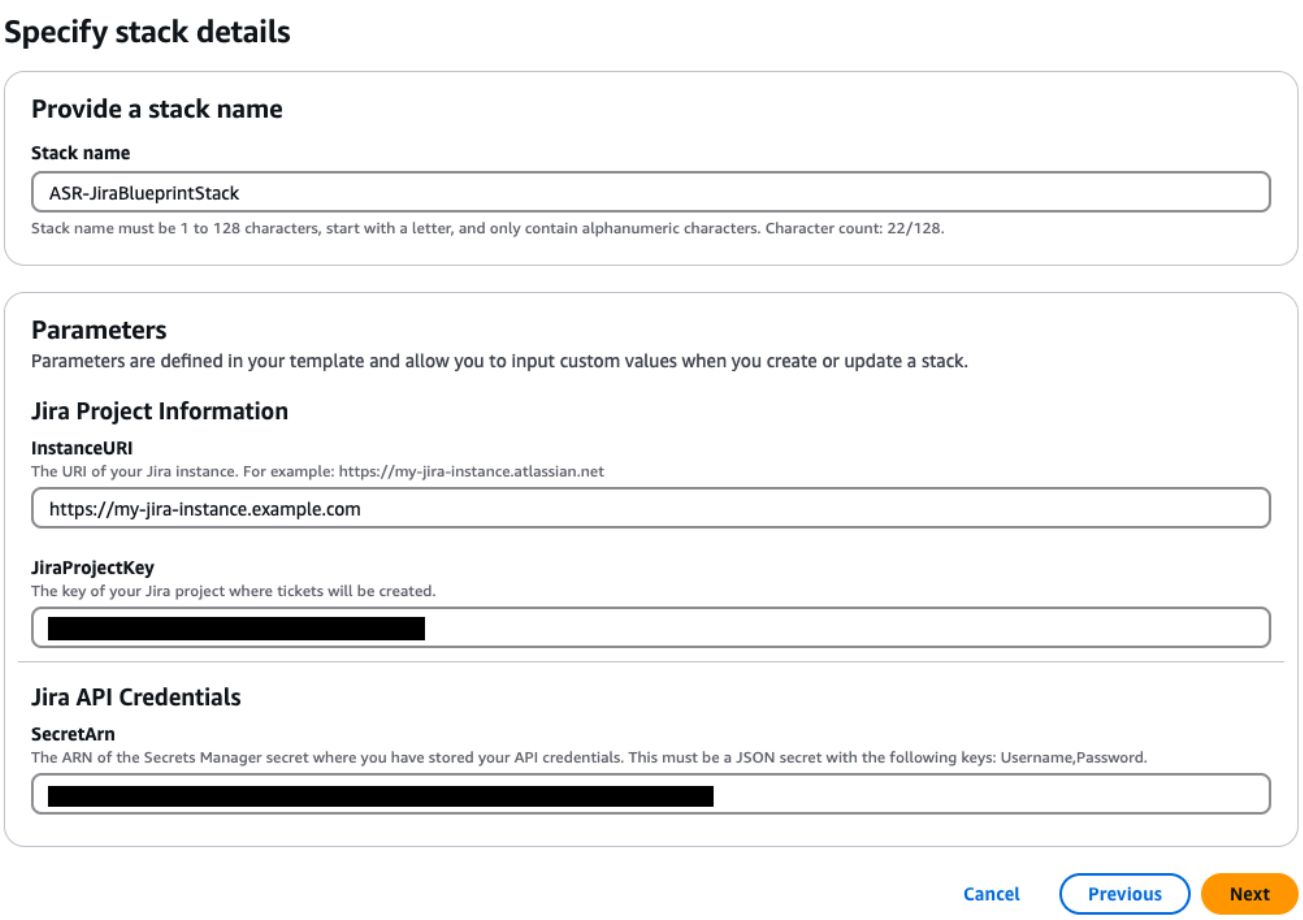
   c. Geben Sie den Projektschlüssel für das Jira-Projekt ein, an das Sie Tickets senden möchten.

   d. Erstellen Sie in Secrets Manager ein neues Key-Value-Secret, das Ihre `Username` Jira und enthält. `Password`

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

   e. Fügen Sie den ARN dieses Geheimnisses als Eingabe zum Stack hinzu.

   Geben Sie einen Stacknamen, Jira-Projektinformationen und Jira-API-Anmeldeinformationen an.



So stellen Sie den ServiceNow Stack bereit:

f. Geben Sie einen Namen für Ihren Stack ein.

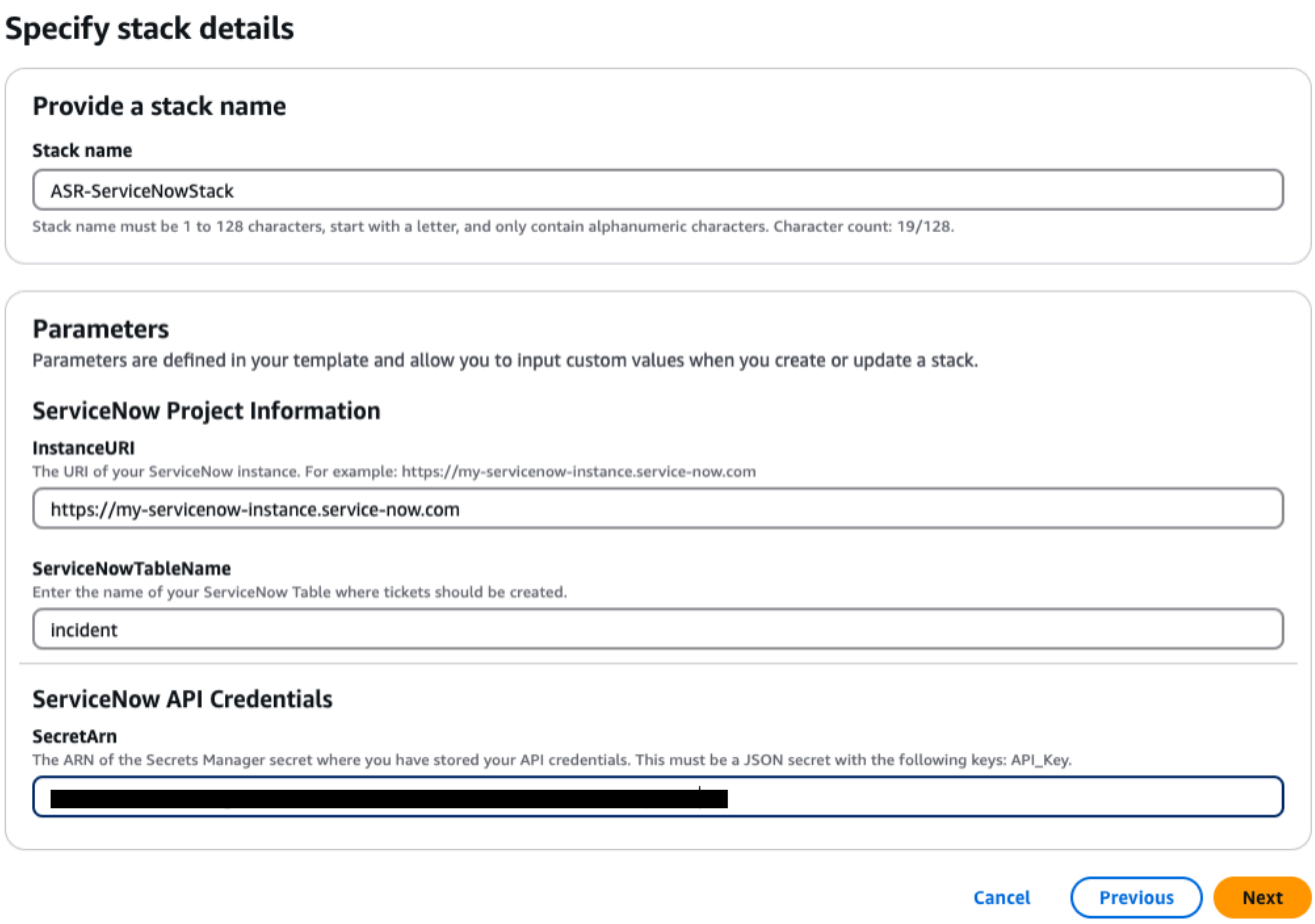
g. Geben Sie den URI Ihrer ServiceNow Instanz an.

h. Geben Sie Ihren ServiceNow Tabellennamen an.

i. Erstellen Sie einen API-Schlüssel ServiceNow mit der Berechtigung, die Tabelle zu ändern, in die Sie schreiben möchten.

j. Erstellen Sie in Secrets Manager ein Geheimnis mit dem Schlüssel `API_Key` und geben Sie den geheimen ARN als Eingabe für den Stack an.

Geben Sie einen Stacknamen, ServiceNow Projektinformationen und ServiceNow API-Anmeldeinformationen an.



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

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

1. Starten Sie den Admin-Stack mit Ihrem Security Hub-Administratorkonto. `automated-security-response-admin.template` In der Regel eines pro Organisation in einer einzigen Region. Da dieser Stack verschachtelte Stacks verwendet, müssen Sie diese Vorlage als selbstverwaltete Vorlage bereitstellen. StackSet

Parameters

Parameter	Standard	Description
Laden Sie den SC Admin Stack	`yes`	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von SC-Steuerelementen installiert werden sollen.
Laden Sie den AFSBP Admin Stack	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von FSBP-Steuerelementen installiert werden sollen.
CIS120 Admin-Stack laden	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von CIS12 0 Kontrollen installiert werden sollen.
CIS140 Admin-Stack laden	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von CIS14 0 Kontrollen installiert werden sollen.
Laden Sie CIS3 00 Admin Stack	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von CIS3 00-Steuerelementen installiert werden sollen.
PC1321 Admin-Stack laden	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von

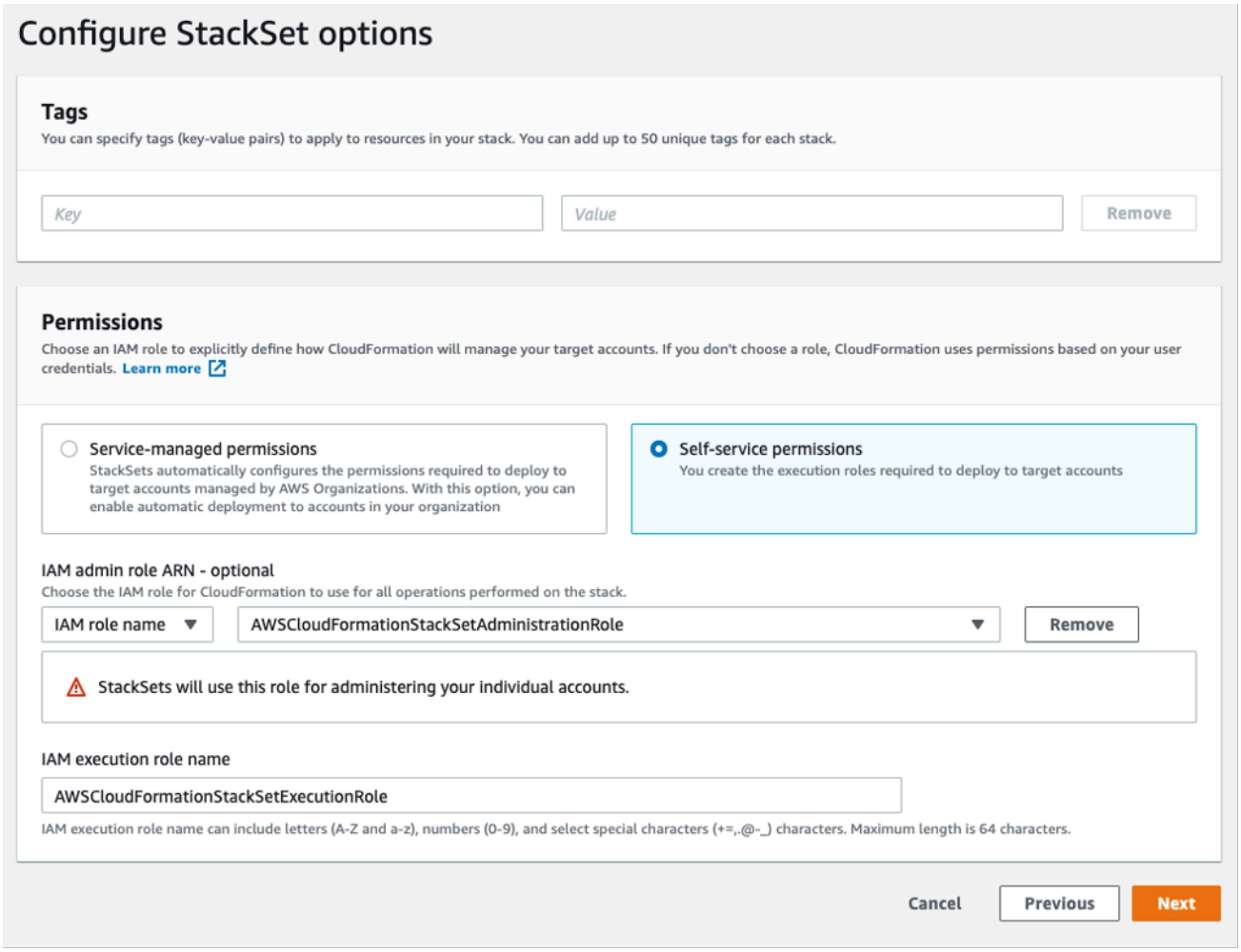
Parameter	Standard	Description
		PC1321 Kontrollen installiert werden sollen.
Laden Sie den NIST Admin Stack	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von NIST-Steuerelementen installiert werden sollen.
Orchestrator-Protokollgruppe wiederverwenden	no	Wählen Sie aus, ob eine vorhandene `S00111-ASR-Orchestrator` CloudWatch Protokollgruppe wiederverwendet werden soll oder nicht. Dies vereinfacht die Neuinstallation und Upgrades, ohne dass Protokolldaten aus einer früheren Version verloren gehen. Bestehende Objekte wiederverwenden`yes`, `Orchestrator Log Group` wählen Sie aus, ob sie `Orchestrator Log Group` noch aus einer früheren Bereitstellung in diesem Konto vorhanden sind, andernfalls`no`. Wenn Sie ein Stack-Update von einer früheren Version als v2.3.0 aus durchführen, wählen Sie `no`

Parameter	Standard	Description
ShouldDeployWebUI	`yes`	Stellen Sie die Web-UI-Komponenten bereit, einschließlich API Gateway, Lambda-Funktionen und CloudFront Verteilung. Wählen Sie „Ja“, um die webbasierte Benutzeroberfläche zur Anzeige der Ergebnisse und des Behebungsstatus zu aktivieren. Wenn Sie sich dafür entscheiden, diese Funktion zu deaktivieren, können Sie mit der benutzerdefinierten Security Hub CSPM-Aktion weiterhin automatische Problembehebungen konfigurieren und Behebungen bei Bedarf ausführen.
AdminUserEmail	(Optionale Eingabe)	E-Mail-Adresse für den ersten Admin-Benutzer. Dieser Benutzer wird vollen Administratorzugriff auf die ASR-Webbenutzeroberfläche haben. Nur erforderlich, wenn die Webbenutzeroberfläche aktiviert ist.
Verwenden Sie CloudWatch Metriken	`yes`	Geben Sie an, ob CloudWatch Metrics für die Überwachung der Lösung aktiviert werden sollen. Dadurch wird ein CloudWatch Dashboard zum Anzeigen von Metriken erstellt.

Parameter	Standard	Description
Verwenden Sie CloudWatch Metrik-Alarme	`yes`	Geben Sie an, ob CloudWatch Metrik-Alarme für die Lösung aktiviert werden sollen. Dadurch werden Alarme für bestimmte von der Lösung erfasste Metriken erstellt.
RemediationFailureAlarmThreshold	`5`	Geben Sie den Schwellenwert für den Prozentsatz der Behebungsfehler pro Kontroll-ID an. Wenn Sie beispielsweise einen Wert eingeben5, erhalten Sie einen Alarm, wenn eine Kontroll-ID an einem bestimmten Tag bei mehr als 5% der Behebungen fehlschlägt. Dieser Parameter funktioniert nur, wenn Alarme erstellt wurden (siehe Parameter „CloudWatch Metrik-Alarme verwenden“).

Parameter	Standard	Description
EnableEnhancedCloudWatchMetrics	no	Wenn `yes`, werden zusätzliche CloudWatch Messwerte erstellt, um die gesamte Steuerung IDs einzeln im CloudWatch Dashboard und als CloudWatch Alarme nachzuverfolgen. Informationen zu den zusätzlichen Kosten, die dadurch entstehen, finden Sie im Abschnitt Kosten.
TicketGenFunctionName	(Optionale Eingabe)	Optional. Lassen Sie das Feld leer, wenn Sie kein Ticketsystem integrieren möchten. Andernfalls geben Sie den Lambda-Funktionsnamen aus der Stack-Ausgabe von Schritt 0 an, zum Beispiel: `SO0111-ASR-ServiceNow-TicketGenerator` .

Optionen konfigurieren StackSet



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

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

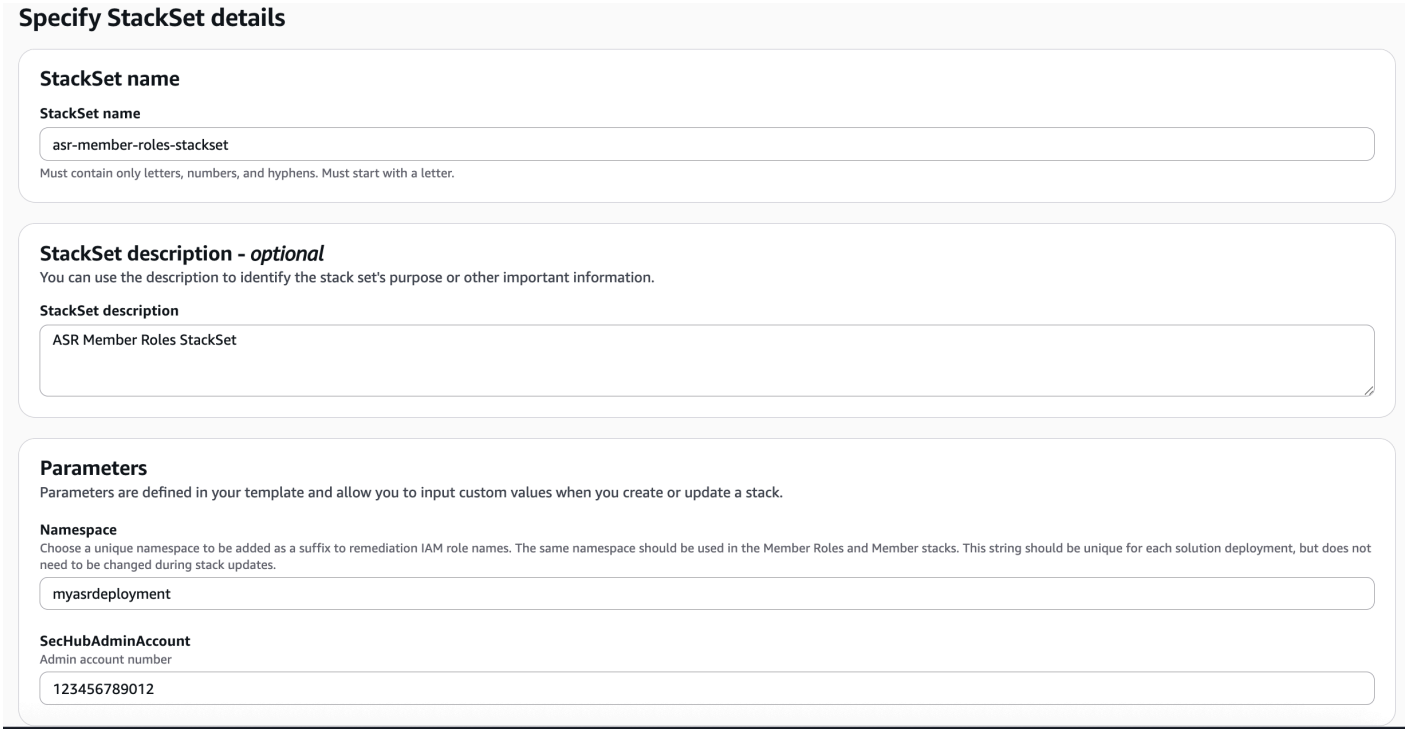
Verwenden Sie einen vom Service verwalteten Dienst StackSets , um die Vorlage für Mitgliederrollen bereitzustellen,. `automated-security-response-member-roles.template` Diese StackSet muss in einer Region pro Mitgliedskonto bereitgestellt werden. Es definiert die globalen Rollen, die kontoübergreifende API-Aufrufe von der ASR Orchestrator-Schrittfunktion aus ermöglichen.

Parameters

Parameter	Standard	Description
Namespace	*<Requires input>*	Geben Sie eine Zeichenfolge mit bis zu 9 alphanumerischen Kleinbuchstaben ein. Eindeutiger Namespace, der als Suffix zu IAM-Rollennamen für die Wartung hinzugefügt werden soll. Derselbe Namespace sollte in den Mitgliedsrollen und Mitgliedsstapeln verwendet werden. Diese Zeichenfolge sollte für jede Lösungsbereitstellung eindeutig sein, muss aber bei Stack-Updates nicht geändert werden. Der Namespace-Wert muss nicht für jedes Mitgliedskonto eindeutig sein.
Sec Hub-Kontoadministrator	*<Requires input>*	Geben Sie die 12-stellige Konto-ID für das AWS Security Hub-Administratorkonto ein. Dieser Wert gewährt der Lösungsrolle des Administratorkontos Berechtigungen.

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

Geben Sie Einzelheiten an StackSet



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

Da der Mitglieds-Stack verschachtelte Stacks verwendet, müssen Sie ihn als selbstverwaltetes System bereitstellen. StackSet Dies unterstützt keine automatische Bereitstellung für neue Konten in der AWS-Organisation.

Parameters

Parameter	Standard	Description
Geben Sie den Namen der LogGroup an, die zur Erstellung von metrischen Filtern und Alarmen verwendet werden sollen	`<Requires input>`	Geben Sie den Namen einer CloudWatch Protokollgruppe an, in der API-Aufrufe CloudTrail protokolliert werden. Dies wird für CIS 3.1-3.14-Korrekturen verwendet.

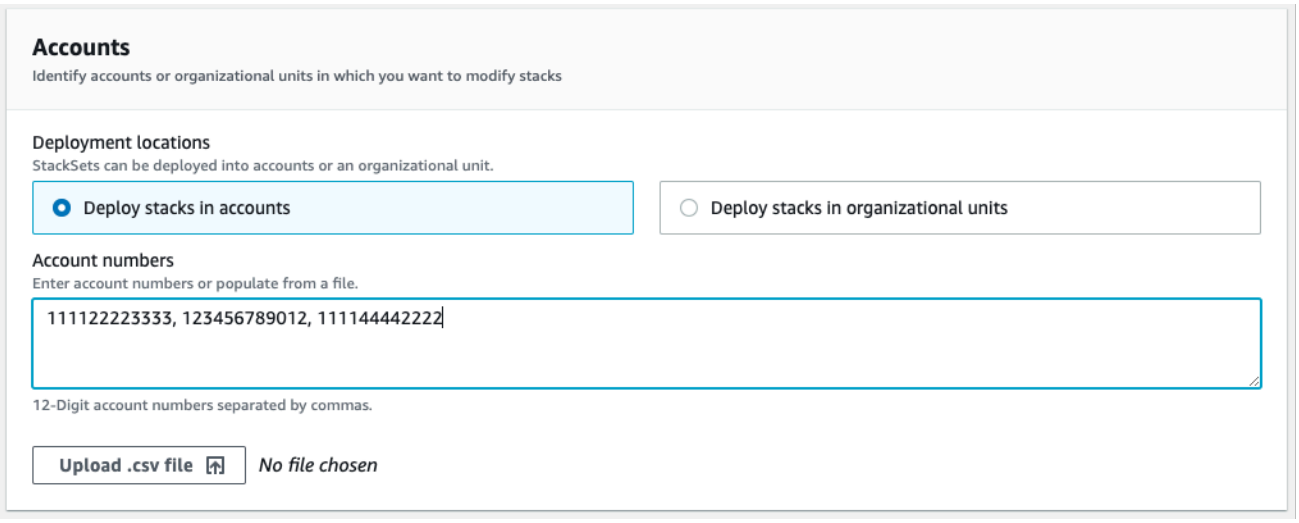
Parameter	Standard	Description
Laden Sie den SC-Mitgliedsstapel	`yes`	Geben Sie an, ob die Mitgliedskomponenten für die automatische Wiederherstellung der SC-Steuerelemente installiert werden sollen.
Laden Sie den AFSBP-Mitgliedsstapel	`no`	Geben Sie an, ob die Mitgliedskomponenten für die automatische Behebung von FSBP-Steuerelementen installiert werden sollen.
Stapel mit CIS12 0 Mitgliedern laden	`no`	Geben Sie an, ob die Mitgliedskomponenten für die automatische Korrektur von CIS12 0 Kontrollen installiert werden sollen.
Stapel mit CIS14 0 Mitgliedern laden	`no`	Geben Sie an, ob die Mitgliedskomponenten für die automatische Korrektur von CIS14 0 Kontrollen installiert werden sollen.
Laden Sie den Stapel mit CIS3 00 Mitgliedern	`no`	Geben Sie an, ob die Mitgliedskomponenten für die automatische Korrektur von CIS3 00-Steuerelementen installiert werden sollen.
PC1321 Mitgliedsstapel laden	`no`	Geben Sie an, ob die Mitgliedskomponenten für die automatische Korrektur von PC1321 Kontrollen installiert werden sollen.

Parameter	Standard	Description
Laden Sie den NIST-Mitg liedsstapel	no	Geben Sie an, ob die Mitgliedskomponenten für die automatische Korrektur von NIST-Kontrollen installiert werden sollen.
S3-Bucket für Redshift Audit Logging erstellen	no	Wählen Sie aus`yes`, ob der S3-Bucket für die FSBP 4.4-Wiederherstellung erstellt werden soll RedShift. Einzelheiten zum S3-Bucket und zur Behebung finden Sie unter Redshift.4-Remediation im AWS Security Hub Hub-Benutzerhandbuch.
Sec Hub-Administratorkonto	*<Requires input>*	Geben Sie die 12-stelli ge Konto-ID für das AWS Security Hub-Administratork onto ein.

Parameter	Standard	Description
Namespace	*<Requires input>*	Geben Sie eine Zeichenfolge mit bis zu 9 alphanumerischen Kleinbuchstaben ein. Diese Zeichenfolge wird Teil der IAM-Rollennamen und des Action Log S3-Buckets. Verwenden Sie denselben Wert für die Bereitstellung des Member-Stacks und die Stack-Bereitstellung der Mitgliedsrollen. Die Zeichenfolge sollte für jede Lösungsbereitstellung eindeutig sein, muss aber bei Stack-Updates nicht geändert werden.

Parameter	Standard	Description
EnableCloudTrailForASRActionProtokoll	no	Wählen Sie aus, `yes` ob Sie die von der Lösung ausgeführten Verwaltungsereignisse im CloudWatch Dashboard überwachen möchten. Die Lösung erstellt in jedem Mitgliedskonto, das Sie auswählen, eine CloudTrail Spur`yes`. Sie müssen die Lösung in einer AWS-Organisation bereitstellen, um diese Funktion zu aktivieren. Darüber hinaus können Sie diese Funktion nur in einer einzigen Region innerhalb desselben Kontos aktivieren. Informationen zu den zusätzlichen Kosten, die dadurch entstehen, finden Sie im Abschnitt Kosten.

Konten



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

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

Automatisierte Bereitstellung — Stacks

> **Note**
>
> Für Kunden mit mehreren Konten empfehlen wir dringend die Bereitstellung mit StackSets.

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

Zeit für die Bereitstellung: Ungefähr 30 Minuten

Voraussetzungen

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

Überblick über die Bereitstellung

Gehen Sie wie folgt vor, um diese Lösung auf AWS bereitzustellen.

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

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

Schritt 1: Starten Sie den Admin-Stack

- Starten Sie die `automated-security-response-admin.template` CloudFormation AWS-Vorlage in Ihrem AWS Security Hub-Administratorkonto.
- Wählen Sie aus, welche Sicherheitsstandards installiert werden sollen.
- Wählen Sie eine vorhandene Orchestrator-Protokollgruppe aus, die verwendet werden soll (wählen Sie aus, `Yes` ob sie `SO0111-ASR-Orchestrator` bereits in einer früheren Installation vorhanden ist).

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

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

Schritt 3: Starten Sie den Member-Stack

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

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

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

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

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

   So stellen Sie den Jira-Stack bereit:

a. Geben Sie einen Namen für Ihren Stack ein.

b. Geben Sie den URI für Ihre Jira-Instanz ein.

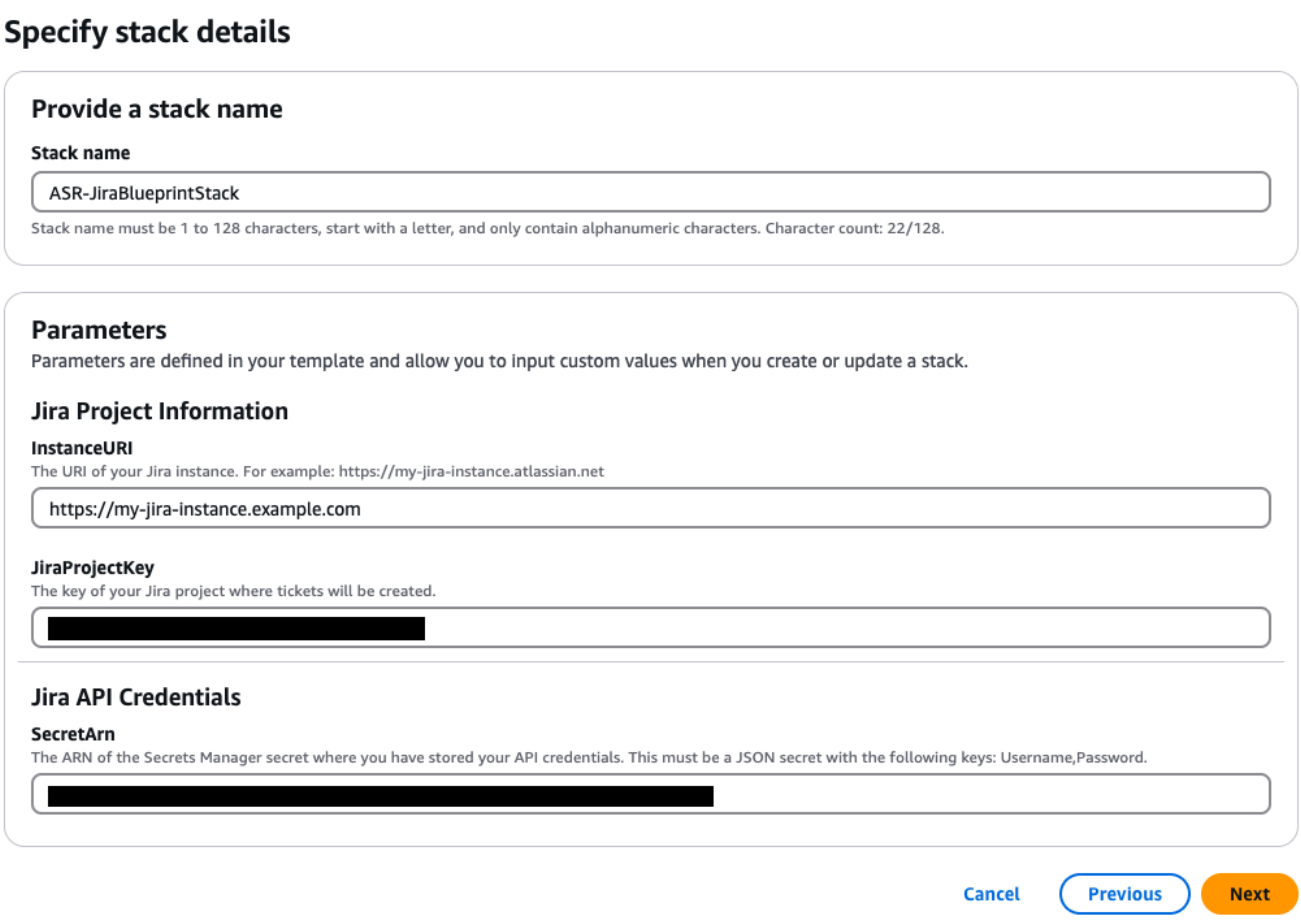
c. Geben Sie den Projektschlüssel für das Jira-Projekt ein, an das Sie Tickets senden möchten.

d. Erstellen Sie in Secrets Manager ein neues Key-Value-Secret, das Ihre `Username` Jira und enthält. `Password`

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

e. Fügen Sie den ARN dieses Geheimnisses als Eingabe zum Stack hinzu.

„Geben Sie einen Stacknamen, Jira-Projektinformationen und Jira-API-Anmeldeinformationen an.



So stellen Sie den ServiceNow Stack bereit:

f. Geben Sie einen Namen für Ihren Stack ein.

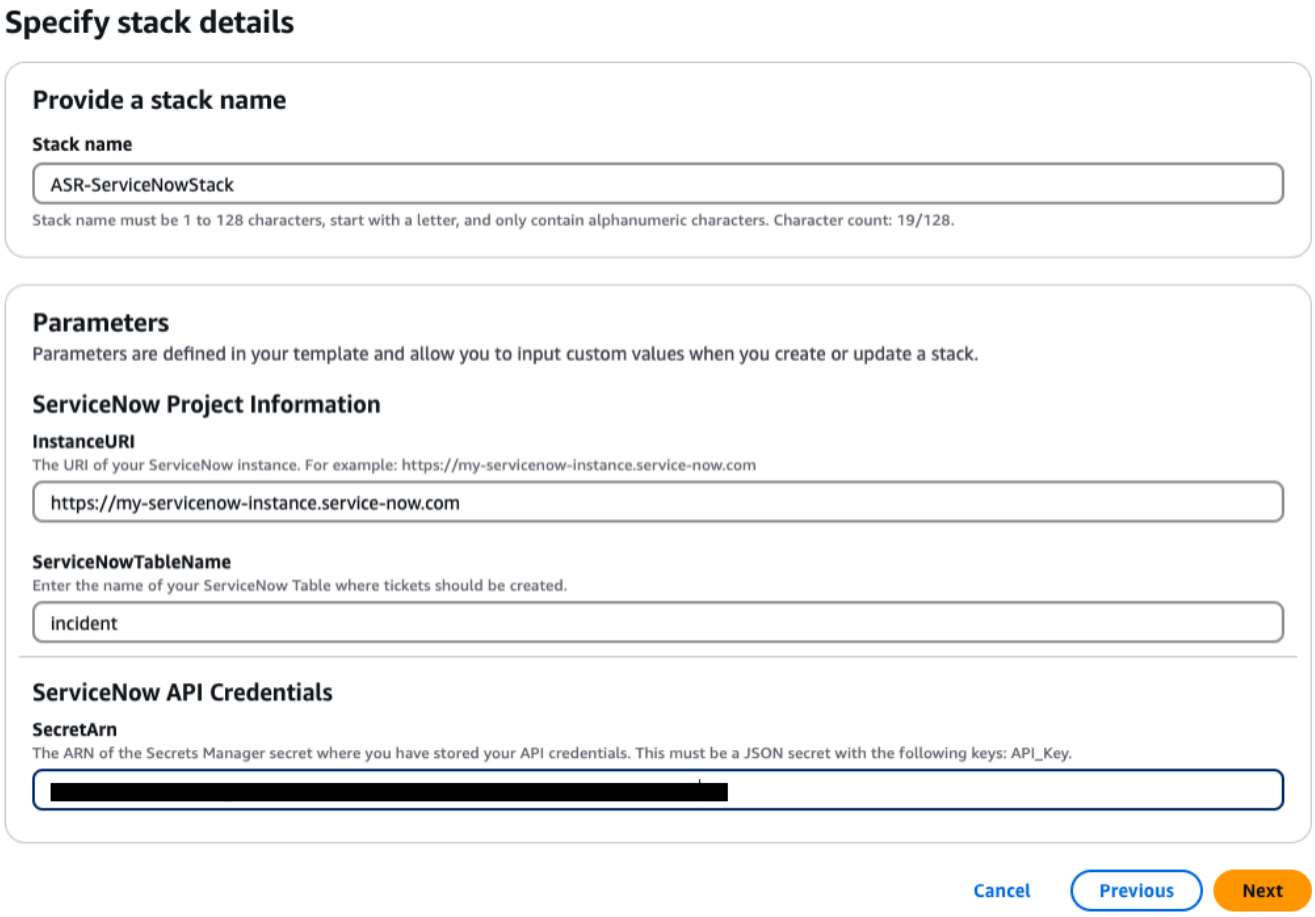
g. Geben Sie den URI Ihrer ServiceNow Instanz an.

h. Geben Sie Ihren ServiceNow Tabellennamen an.

i. Erstellen Sie einen API-Schlüssel ServiceNow mit der Berechtigung, die Tabelle zu ändern, in die Sie schreiben möchten.

j. Erstellen Sie in Secrets Manager ein Geheimnis mit dem Schlüssel `API_Key` und geben Sie den geheimen ARN als Eingabe für den Stack an.

Geben Sie einen Stacknamen, ServiceNow Projektinformationen und ServiceNow API-Anmeldeinformationen an.



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

Schritt 1: Starten Sie den Admin-Stack

> **Important**
>
> Diese Lösung beinhaltet die Datenerfassung. Wir verwenden diese Daten, um besser zu verstehen, wie Kunden diese Lösung und die damit verbundenen Services und Produkte nutzen. AWS ist Eigentümer der im Rahmen dieser Umfrage gesammelten Daten. Die Datenerfassung unterliegt dem AWS-Datenschutzhinweis.

Diese automatisierte CloudFormation AWS-Vorlage stellt die Automated Security Response on AWS-Lösung in der AWS-Cloud bereit. Bevor Sie den Stack starten, müssen Sie Security Hub aktivieren und die Voraussetzungen erfüllen.

> **Note**
>
> Sie sind für die Kosten der AWS-Services verantwortlich, die Sie beim Betrieb dieser Lösung in Anspruch nehmen. Weitere Informationen finden Sie im Abschnitt Kosten in diesem Handbuch und auf der Preisseite für jeden AWS-Service, der in dieser Lösung verwendet wird.

1. Melden Sie sich von dem Konto aus, in dem der AWS Security Hub derzeit konfiguriert ist, bei der AWS-Managementkonsole an, und verwenden Sie die Schaltfläche unten, um die `automated-security-response-admin.template` CloudFormation AWS-Vorlage zu starten.

   Launch solution

   Sie können auch die Vorlage herunterladen als Ausgangspunkt für eine eigene Implementierung verwenden.

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

> **Note**
>
> Diese Lösung verwendet AWS Systems Manager, der derzeit nur in bestimmten AWS-Regionen verfügbar ist. Die Lösung funktioniert in allen Regionen, die diesen Service unterstützen. Die aktuelle Verfügbarkeit nach Regionen finden Sie in der Liste der regionalen AWS-Dienste.

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

Parameter	Standard	Description
Laden Sie den SC Admin Stack	`yes`	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von SC-Steuerelementen installiert werden sollen.
Laden Sie den AFSBP Admin Stack	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von FSBP-Steuerelementen installiert werden sollen.
CIS120 Admin-Stack laden	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von CIS12 0 Kontrollen installiert werden sollen.
CIS140 Admin-Stack laden	no	Geben Sie an, ob die Admin-Komponenten für die

Parameter	Standard	Description
		automatische Korrektur von CIS14 0 Kontrollen installiert werden sollen.
Laden Sie CIS3 00 Admin Stack	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von CIS3 00-Steuerelementen installiert werden sollen.
PC1321 Admin-Stack laden	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von PC1321 Kontrollen installiert werden sollen.
Laden Sie den NIST Admin Stack	no	Geben Sie an, ob die Admin-Komponenten für die automatische Korrektur von NIST-Steuerelementen installiert werden sollen.

Parameter	Standard	Description
Orchestrator-Protokollgruppe wiederverwenden	`no`	Wählen Sie aus, ob eine vorhandene `SO0111-ASR-Orchestrator` CloudWatch Protokoll gruppe wiederverwendet werden soll oder nicht. Dies vereinfacht die Neuinstal lation und Upgrades, ohne dass Protokolldaten aus einer früheren Version verloren gehen. Bestehende Objekte wiederverwenden`yes`, `Orchestrator Log Group` wählen Sie aus, ob sie `Orchestrator Log Group` noch aus einer früheren Bereitstellung in diesem Konto vorhanden sind, andernfalls`no`. Wenn Sie ein Stack-Update von einer früheren Version als v2.3.0 aus durchführen, wählen Sie no
ShouldDeployWebUI	`yes`	Stellen Sie die Web-UI-Ko mponenten bereit, einschlie ßlich API Gateway, Lambda-Funktionen und CloudFron t Verteilung. Wählen Sie „Ja“, um das webbasierte Dashboard zur Anzeige der Ergebnisse und des Behebungsstatus zu aktiviere n.

Parameter	Standard	Description
AdminUserEmail	(Optionale Eingabe)	E-Mail-Adresse für den ersten Admin-Benutzer. Dieser Benutzer wird vollen Administratorzugriff auf die ASR-Webbenutzeroberfläche haben. Nur erforderlich, wenn die Webbenutzeroberfläche aktiviert ist.
Verwenden Sie CloudWatch Metriken	`yes`	Geben Sie an, ob CloudWatch Metrics für die Überwachung der Lösung aktiviert werden sollen. Dadurch wird ein CloudWatch Dashboard zum Anzeigen von Metriken erstellt.
Verwenden Sie CloudWatch Metrik-Alarme	`yes`	Geben Sie an, ob CloudWatch Metrik-Alarme für die Lösung aktiviert werden sollen. Dadurch werden Alarme für bestimmte von der Lösung erfasste Metriken erstellt.

Parameter	Standard	Description
RemediationFailureAlarmThreshold	5	Geben Sie den Schwellenwert für den Prozentsatz der Behebungsfehler pro Kontroll-ID an. Wenn Sie beispielsweise einen Wert eingeben5, erhalten Sie einen Alarm, wenn eine Kontroll-ID an einem bestimmten Tag bei mehr als 5% der Behebungen fehlschlägt. Dieser Parameter funktioniert nur, wenn Alarme erstellt wurden (siehe Parameter „CloudWatch Metrik-Alarme verwenden“).
EnableEnhancedCloudWatchMetrics	no	Wennyes, werden zusätzliche CloudWatch Messwerte erstellt, um die gesamte Steuerung IDs einzeln im CloudWatch Dashboard und als CloudWatch Alarme nachzuverfolgen. Informationen zu den zusätzlichen Kosten, die dadurch entstehen, finden Sie im Abschnitt Kosten.

Parameter	Standard	Description
TicketGenFunctionName	(Optionale Eingabe)	Optional. Lassen Sie das Feld leer, wenn Sie kein Ticketsystem integrieren möchten. Andernfalls geben Sie den Lambda-Funktionsnamen aus der Stack-Ausgabe von Schritt 0 an, zum Beispiel: `SO0111-ASR-ServiceNow-TicketGenerator` .

> **Note**
>
> Sie müssen automatische Problembehebungen im Admin-Konto manuell aktivieren, nachdem Sie die Stacks der Lösung bereitgestellt oder aktualisiert haben. CloudFormation

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

Sie können den Status des Stacks in der CloudFormation AWS-Konsole in der Spalte Status anzeigen. Sie sollten in etwa 15 Minuten den Status CREATE_COMPLETE erhalten.

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

Die `automated-security-response-member-roles.template` StackSet dürfen nur in einer Region pro Mitgliedskonto bereitgestellt werden. Es definiert die globalen Rollen, die kontoübergreifende API-Aufrufe über die ASR Orchestrator-Schrittfunktion ermöglichen.

1. Melden Sie sich bei der AWS-Managementkonsole für jedes AWS Security Hub-Mitgliedskonto an (einschließlich des Administratorkontos, das ebenfalls Mitglied ist). Wählen Sie die Schaltfläche, um die `automated-security-response-member-roles.template` CloudFormation AWS-Vorlage zu starten. Sie können auch die Vorlage herunterladen als Ausgangspunkt für eine eigene Implementierung verwenden.

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

Parameter	Standard	Description
Namespace	*<Requires input>*	Geben Sie eine Zeichenfolge mit bis zu 9 alphanumerischen Kleinbuchstaben ein. Eindeutiger Namespace, der als Suffix zu IAM-Rollennamen für die Wartung hinzugefügt werden soll. Derselbe Namespace sollte in den Mitgliedsrollen und Mitgliedsstapeln verwendet werden. Diese Zeichenfolge sollte für jede Lösungsbereitstellung eindeutig sein, muss aber bei Stack-Updates nicht geändert werden. Der Namespace-Wert muss

Parameter	Standard	Description
		nicht für jedes Mitgliedskonto eindeutig sein.
Sec Hub-Kontoadministrator	`<Requires input>`	Geben Sie die 12-stellige Konto-ID für das AWS Security Hub-Administratorkonto ein. Dieser Wert gewährt der Lösungsrolle des Administratorkontos Berechtigungen.

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

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

Schritt 3: Starten Sie den Member-Stack

> **Important**
>
> Diese Lösung beinhaltet die Datenerfassung. Wir verwenden diese Daten, um besser zu verstehen, wie Kunden diese Lösung und die damit verbundenen Services und Produkte nutzen. AWS ist Eigentümer der im Rahmen dieser Umfrage gesammelten Daten. Die Datenerfassung unterliegt der AWS-Datenschutzrichtlinie.

Der `automated-security-response-member` Stack muss in jedem Security Hub-Mitgliedskonto installiert werden. Dieser Stack definiert die Runbooks für die automatisierte Problembehebung. Der

Administrator jedes Mitgliedskontos kann kontrollieren, welche Abhilfemaßnahmen über diesen Stack verfügbar sind.

1. Melden Sie sich bei der AWS-Managementkonsole für jedes AWS Security Hub-Mitgliedskonto an (einschließlich des Administratorkontos, das ebenfalls Mitglied ist). Wählen Sie die Schaltfläche, um die `automated-security-response-member.template` CloudFormation AWS-Vorlage zu starten.

   Launch solution

Sie können die Vorlage auch als Ausgangspunkt für Ihre eigene Implementierung herunterladen. Die Vorlage wird standardmäßig in der Region USA Ost (Nord-Virginia) gestartet. Um diese Lösung in einer anderen AWS-Region zu starten, verwenden Sie die Regionsauswahl in der Navigationsleiste der AWS-Managementkonsole.

+

> **Note**
>
> Diese Lösung verwendet AWS Systems Manager, der derzeit in den meisten AWS-Regionen verfügbar ist. Die Lösung funktioniert in allen Regionen, die diese Services unterstützen. Die aktuelle Verfügbarkeit nach Regionen finden Sie in der Liste der regionalen AWS-Dienste.

1. Vergewissern Sie sich auf der Seite Stack erstellen, dass sich die richtige Vorlagen-URL im Textfeld Amazon S3 S3-URL befindet, und wählen Sie dann Weiter aus.
2. Weisen Sie Ihrem Lösungsstapel auf der Seite „Stack-Details angeben“ einen Namen zu. Informationen zu Einschränkungen bei der Benennung von Zeichen finden Sie unter IAM- und STS-Beschränkungen im AWS Identity and Access Management-Benutzerhandbuch.
3. Geben Sie auf der Seite Parameter die folgenden Parameter an und wählen Sie Weiter.

Parameter	Standard	Description
Geben Sie den Namen der LogGroup an, die zur Erstellung von metrische	*<Requires input>*	Geben Sie den Namen einer CloudWatch Protokoll gruppe an, in der API-

Parameter	Standard	Description
n Filtern und Alarmen verwendet werden sollen		Aufrufe CloudTrail protokoll iert werden. Dies wird für CIS 3.1-3.14-Korrekturen verwendet.
Laden Sie den SC-Mitgli edsstapel	`yes`	Geben Sie an, ob die Mitgliedskomponenten für die automatische Wiederher stellung der SC-Steuer elemente installiert werden sollen.
Laden Sie den AFSBP-Mit gliedsstapel	no	Geben Sie an, ob die Mitgliedskomponenten für die automatische Behebung von FSBP-Steuerelementen installiert werden sollen.
Stapel mit CIS12 0 Mitgliede rn laden	no	Geben Sie an, ob die Mitgliedskomponenten für die automatische Korrektur von CIS12 0 Kontrollen installiert werden sollen.
Stapel mit CIS14 0 Mitgliede rn laden	no	Geben Sie an, ob die Mitgliedskomponenten für die automatische Korrektur von CIS14 0 Kontrollen installiert werden sollen.
Laden Sie den Stapel mit CIS3 00 Mitgliedern	no	Geben Sie an, ob die Mitgliedskomponenten für die automatische Korrektur von CIS3 00-Steuerelementen installiert werden sollen.

Parameter	Standard	Description
PC1321 Mitgliedsstapel laden	no	Geben Sie an, ob die Mitgliedskomponenten für die automatische Korrektur von PC1321 Kontrollen installiert werden sollen.
Laden Sie den NIST-Mitg liedsstapel	no	Geben Sie an, ob die Mitgliedskomponenten für die automatische Korrektur von NIST-Kontrollen installiert werden sollen.
S3-Bucket für Redshift Audit Logging erstellen	no	Wählen Sie aus`yes`, ob der S3-Bucket für die FSBP 4.4-Wiederherstellung erstellt werden soll RedShift. Einzelheiten zum S3-Bucket und zur Behebung finden Sie unter Redshift.4-Remediation im AWS Security Hub Hub-Benutzerhandbuch.
Sec Hub-Administratorkonto	*<Requires input>*	Geben Sie die 12-stelli ge Konto-ID für das AWS Security Hub-Administratork onto ein.

Parameter	Standard	Description
Namespace	*<Requires input>*	Geben Sie eine Zeichenfolge mit bis zu 9 alphanumerischen Kleinbuchstaben ein. Diese Zeichenfolge wird Teil der IAM-Rollennamen und des Action Log S3-Buckets. Verwenden Sie denselben Wert für die Bereitstellung des Member-Stacks und die Stack-Bereitstellung der Mitgliedsrollen. Die Zeichenfolge sollte für jede Lösungsbereitstellung eindeutig sein, muss aber bei Stack-Updates nicht geändert werden.

Parameter	Standard	Description
EnableCloudTrailFo rASRActionProtokoll	no	Wählen Sie aus, `yes` ob Sie die von der Lösung ausgeführten Verwaltun gsereignisse im CloudWatc h Dashboard überwachen möchten. Die Lösung erstellt in jedem Mitgliedskonto, das Sie auswählen, eine CloudTrail Spur`yes`. Sie müssen die Lösung in einer AWS-Organisation bereitste llen, um diese Funktion zu aktivieren. Darüber hinaus können Sie diese Funktion nur in einer einzigen Region innerhalb desselben Kontos aktivieren. Informationen zu den zusätzlichen Kosten, die dadurch entstehen, finden Sie im Abschnitt Kosten.

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

Sie können den Status des Stacks in der CloudFormation AWS-Konsole in der Spalte Status anzeigen. Sie sollten in etwa 15 Minuten den Status CREATE_COMPLETE erhalten.

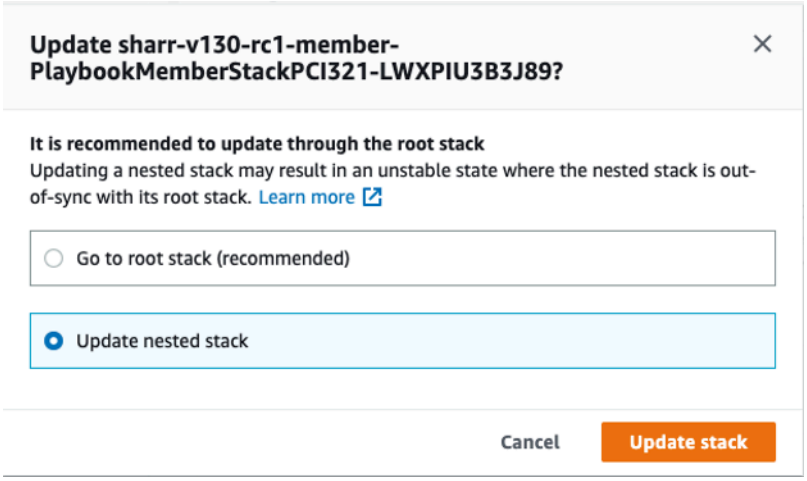
Schritt 4: (Optional) Passen Sie die verfügbaren Abhilfemaßnahmen an

Wenn Sie bestimmte Abhilfemaßnahmen aus einem Mitgliedskonto entfernen möchten, können Sie dies tun, indem Sie den verschachtelten Stack entsprechend dem Sicherheitsstandard aktualisieren.

Der Einfachheit halber werden die Optionen für verschachtelte Stacks nicht an den Root-Stack weitergegeben.

1. Melden Sie sich bei der CloudFormation AWS-Konsole an und wählen Sie den verschachtelten Stack aus.
2. Wählen Sie Aktualisieren aus.
3. Wählen Sie Verschachtelten Stack aktualisieren und anschließend Stack aktualisieren aus.

   Verschachtelten Stapel aktualisieren



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

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

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

Sie können den Status des Stacks in der CloudFormation AWS-Konsole in der Spalte Status anzeigen. Sie sollten in etwa 15 Minuten den Status CREATE_COMPLETE erhalten.

Einsatz des Control Tower (CT)

Der Leitfaden Customizations for AWS Control Tower (cFCT) richtet sich an Administratoren, DevOps Fachleute, unabhängige Softwareanbieter, IT-Infrastrukturarchitekten und Systemintegratoren, die ihre AWS Control Tower Tower-Umgebungen für ihr Unternehmen und ihre Kunden anpassen und erweitern möchten. Es enthält Informationen zur Anpassung und Erweiterung der AWS Control Tower Tower-Umgebung mit dem cFCT-Anpassungspaket.

Zeit für die Bereitstellung: Ungefähr 30 Minuten

Voraussetzungen

Stellen Sie vor der Bereitstellung dieser Lösung sicher, dass sie für AWS Control Tower Tower-Administratoren vorgesehen ist.

Wenn Sie bereit sind, Ihre landing zone mit der AWS Control Tower Tower-Konsole einzurichten APIs, oder gehen Sie wie folgt vor:

Informationen zu den ersten Schritten mit AWS Control Tower finden Sie unter: Erste Schritte mit AWS Control Tower

Informationen zum Anpassen Ihrer landing zone finden Sie unter: Anpassen Ihrer Landezone

Informationen zum Starten und Bereitstellen Ihrer landing zone finden Sie unter: Leitfaden zur Bereitstellung von Landezonen

Überblick über den Einsatz

Gehen Sie wie folgt vor, um diese Lösung auf AWS bereitzustellen.

Schritt 1: S3-Bucket erstellen und bereitstellen

> **Note**
>
> S3-Bucket-Konfiguration — nur für ADMIN. Dies ist ein einmaliger Einrichtungsschritt und sollte von Endbenutzern nicht wiederholt werden. Die S3-Buckets speichern das

Bereitstellungspaket, einschließlich der CloudFormation AWS-Vorlage und des Lambda-Codes, die für die Ausführung von ASR erforderlich sind. Diese Ressourcen werden mit oder bereitgestellt. CfCt StackSet

1. Konfigurieren Sie den S3-Bucket

Richten Sie den S3-Bucket ein, der zum Speichern und Bereitstellen Ihrer Bereitstellungspakete verwendet wird.

2. Einrichten der -Umgebung

Bereiten Sie die erforderlichen Umgebungsvariablen, Anmeldeinformationen und Tools vor, die für den Build- und Bereitstellungsprozess erforderlich sind.

3. Konfigurieren Sie S3-Bucket-Richtlinien

Definieren und wenden Sie die entsprechenden Bucket-Richtlinien an, um den Zugriff und die Berechtigungen zu kontrollieren.

4. Bereiten Sie den Build vor

Kompilieren, verpacken oder bereiten Sie Ihre Anwendung oder Ressourcen auf andere Weise für die Bereitstellung vor.

5. Stellen Sie Pakete auf S3 bereit

Laden Sie die vorbereiteten Build-Artefakte in den dafür vorgesehenen S3-Bucket hoch.

Schritt 2: Stack-Bereitstellung auf AWS Control Tower

1. Erstellen Sie ein Build-Manifest für ASR-Komponenten

Definieren Sie ein Build-Manifest, das alle ASR-Komponenten, ihre Versionen, Abhängigkeiten und Build-Anweisungen auflistet.

2. Aktualisieren Sie das CodePipeline

Ändern Sie die CodePipeline AWS-Konfiguration so, dass sie die neuen Build-Schritte, Artefakte oder Stufen enthält, die für die Bereitstellung der ASR-Komponenten erforderlich sind.

Schritt 1: Erstellen und Bereitstellen im S3-Bucket

AWS-Lösungen verwenden zwei Buckets: einen Bucket für den globalen Zugriff auf Vorlagen, auf den über HTTPS zugegriffen wird, und regionale Buckets für den Zugriff auf Ressourcen innerhalb der Region, wie z. B. Lambda-Code.

1. Konfigurieren Sie den S3-Bucket

Wählen Sie einen eindeutigen Bucket-Namen, z. B. asr-staging. Legen Sie zwei Umgebungsvariablen auf Ihrem Terminal fest. Eine sollte der Basis-Bucket-Name mit -reference als Suffix sein, die andere mit der gewünschten Einsatzregion als Suffix:

```
export BASE_BUCKET_NAME=asr-staging-$(date +%s)
export TEMPLATE_BUCKET_NAME=$BASE_BUCKET_NAME-reference
export REGION=us-east-1
export ASSET_BUCKET_NAME=$BASE_BUCKET_NAME-$REGION
```

2. Einrichtung der Umgebung

Erstellen Sie in Ihrem AWS-Konto zwei Buckets mit diesen Namen, z. B. asr-staging-reference und asr-staging-us-east -1. (Der Referenz-Bucket enthält die CloudFormation Vorlagen, der regionale Bucket enthält alle anderen Assets wie das Lambda-Code-Bundle.) Ihre Buckets sollten verschlüsselt sein und keinen öffentlichen Zugriff zulassen

```
aws s3 mb s3://$TEMPLATE_BUCKET_NAME/
aws s3 mb s3://$ASSET_BUCKET_NAME/
```

> **Note**
>
> Achten Sie bei der Erstellung Ihrer Buckets darauf, dass sie nicht öffentlich zugänglich sind. Verwenden Sie zufällige Bucket-Namen. Deaktivieren Sie den öffentlichen Zugriff. Verwenden Sie die KMS-Verschlüsselung. Und überprüfen Sie vor dem Hochladen, ob Sie den Bucket besitzen.

3. Einrichtung der S3-Buckets-Richtlinie

Aktualisieren Sie die S3-Bucket-Richtlinie $TEMPLATE_BUCKET_NAME so, dass sie die Berechtigungen für die Ausführungskonto-ID enthält PutObject . Weisen Sie diese Berechtigung einer

IAM-Rolle innerhalb des Execute-Kontos zu, die berechtigt ist, in den Bucket zu schreiben. Durch diese Konfiguration können Sie vermeiden, dass der Bucket im Verwaltungskonto erstellt wird.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::template-bucket-name/*",
                "arn:aws:s3:::template-bucket-name"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "org-id"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::template-bucket-name/*",
                "arn:aws:s3:::template-bucket-name"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::account-id:role/iam-role-name"
                }
            }
        }
    ]
}
```

Ändern Sie die Asset-S3-Bucket-Richtlinie so, dass sie Berechtigungen einbezieht. Weisen Sie diese Berechtigung einer IAM-Rolle innerhalb des Execute-Kontos zu, das berechtigt ist, in den Bucket zu schreiben. Wiederholen Sie dieses Setup für jeden regionalen Asset-Bucket (z. B. asr-staging-us-east -1, asr-staging-eu-west -1 usw.), sodass Bereitstellungen in mehreren Regionen möglich sind, ohne dass die Buckets im Management-Konto erstellt werden müssen.

4. Vorbereitung des Builds

- Voraussetzungen:
  - AWS-CLI Version 2
  - Python 3.11+ mit Pip
  - AWS CDK 2.171.1+
  - Node.js 20+ mit npm
  - Poetry v2 mit Plugin zum Exportieren
- Git-Klon https://github.com/aws-solutions/automated-security-response-on-aws.git

Stellen Sie zunächst sicher, dass Sie npm install im Quellordner ausgeführt haben.

Führen Sie als Nächstes im Bereitstellungsordner in Ihrem geklonten Repo build-s3-dist.sh aus und übergeben Sie dabei den Stammnamen Ihres Buckets (z. B. mybucket) und die Version, die Sie erstellen (z. B. v1.0.0). Wir empfehlen, eine Semver-Version zu verwenden, die auf der heruntergeladenen Version basiert (z. B. GitHub GitHub: v1.0.0, dein Build: v1.0.0.mybuild)

```
chmod +x build-s3-dist.sh
export SOLUTION_NAME=automated-security-response-on-aws
export SOLUTION_VERSION=v1.0.0.mybuild
./build-s3-dist.sh -b $BASE_BUCKET_NAME -v $SOLUTION_VERSION
```

5. Pakete auf S3 bereitstellen

```
cd deployment
aws s3 cp global-s3-assets/  s3://$TEMPLATE_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive --acl bucket-owner-full-control
aws s3 cp regional-s3-assets/  s3://$ASSET_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive --acl bucket-owner-full-control
```

Schritt 2: Stack-Bereitstellung auf AWS Control Tower

1. Erstellen Sie ein Manifest für ASR-Komponenten

Nachdem Sie ASR-Artefakte in den S3-Buckets bereitgestellt haben, aktualisieren Sie das Control Tower Tower-Pipeline-Manifest, sodass es auf die neue Version verweist, und lösen Sie dann den Pipeline-Lauf aus, siehe: Controltower-Bereitstellung

> **Important**
>
> Um die korrekte Bereitstellung der ASR-Lösung sicherzustellen, finden Sie in der offiziellen AWS-Dokumentation detaillierte Informationen zur Übersicht der CloudFormation Vorlagen und zur Beschreibung der Parameter. Links zu den Informationen finden Sie unten: Leitfaden zur Übersicht über die Parameter der CloudFormation Vorlagen

Das Manifest für die ASR-Komponenten sieht wie folgt aus:

```
region: us-east-1 #<HOME_REGION_NAME>
version: 2021-03-15

# Control Tower Custom CloudFormation Resources
resources:
  - name: <ADMIN STACK NAME>
    resource_file: s3://<ADMIN TEMPLATE BUCKET path>
    parameters:
      - parameter_key: UseCloudWatchMetricsAlarms
        parameter_value: "yes"
      - parameter_key: TicketGenFunctionName
        parameter_value: ""
      - parameter_key: ShouldDeployWebUI
        parameter_value: "yes"
      - parameter_key: AdminUserEmail
        parameter_value: "<YOUR EMAIL ADDRESS>"
      - parameter_key: LoadSCAdminStack
        parameter_value: "yes"
      - parameter_key: LoadCIS120AdminStack
        parameter_value: "no"
      - parameter_key: LoadCIS300AdminStack
        parameter_value: "no"
      - parameter_key: UseCloudWatchMetrics
        parameter_value: "yes"
      - parameter_key: LoadNIST80053AdminStack
        parameter_value: "no"
      - parameter_key: LoadCIS140AdminStack
        parameter_value: "no"
      - parameter_key: ReuseOrchestratorLogGroup
        parameter_value: "yes"
      - parameter_key: LoadPCI321AdminStack
        parameter_value: "no"
```

```
      - parameter_key: RemediationFailureAlarmThreshold
        parameter_value: "5"
      - parameter_key: LoadAFSBPAdminStack
        parameter_value: "no"
      - parameter_key: EnableEnhancedCloudWatchMetrics
        parameter_value: "no"
    deploy_method: stack_set
    deployment_targets:
     accounts: # :type: list
        - <ACCOUNT_NAME> # and/or
        - <ACCOUNT_NUMBER>
    regions:
      - <REGION_NAME>

  - name:  <ROLE MEMBER STACK NAME>
    resource_file: s3://<ROLE MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: Namespace
        parameter_value: <NAMESPACE>
    deploy_method: stack_set
    deployment_targets:
      organizational_units:
        - <ORG UNIT>

  - name:  <MEMBER STACK NAME>
    resource_file: s3://<MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: LoadCIS120MemberStack
        parameter_value: "no"
      - parameter_key: LoadNIST80053MemberStack
        parameter_value: "no"
      - parameter_key: Namespace
        parameter_value: <NAMESPACE>
      - parameter_key: CreateS3BucketForRedshiftAuditLogging
        parameter_value: "no"
      - parameter_key: LoadAFSBPMemberStack
        parameter_value: "no"
      - parameter_key: LoadSCMemberStack
        parameter_value: "yes"
      - parameter_key: LoadPCI321MemberStack
```

```
        parameter_value: "no"
      - parameter_key: LoadCIS140MemberStack
        parameter_value: "no"
      - parameter_key: EnableCloudTrailForASRActionLog
        parameter_value: "no"
      - parameter_key: LogGroupName
        parameter_value: <LOG_GROUP_NAME>
      - parameter_key: LoadCIS300MemberStack
        parameter_value: "no"
    deploy_method: stack_set
    deployment_targets:
     accounts: # :type: list
        - <ACCOUNT_NAME> # and/or
        - <ACCOUNT_NUMBER>
    organizational_units:
      - <ORG UNIT>
    regions: # :type: list
      - <REGION_NAME>
```

2. Aktualisierung der Code-Pipeline

Fügen Sie einer custom-control-tower-configuration ZIP-Datei eine Manifestdatei hinzu und führen Sie eine aus CodePipeline, siehe: Code-Pipeline-Übersicht

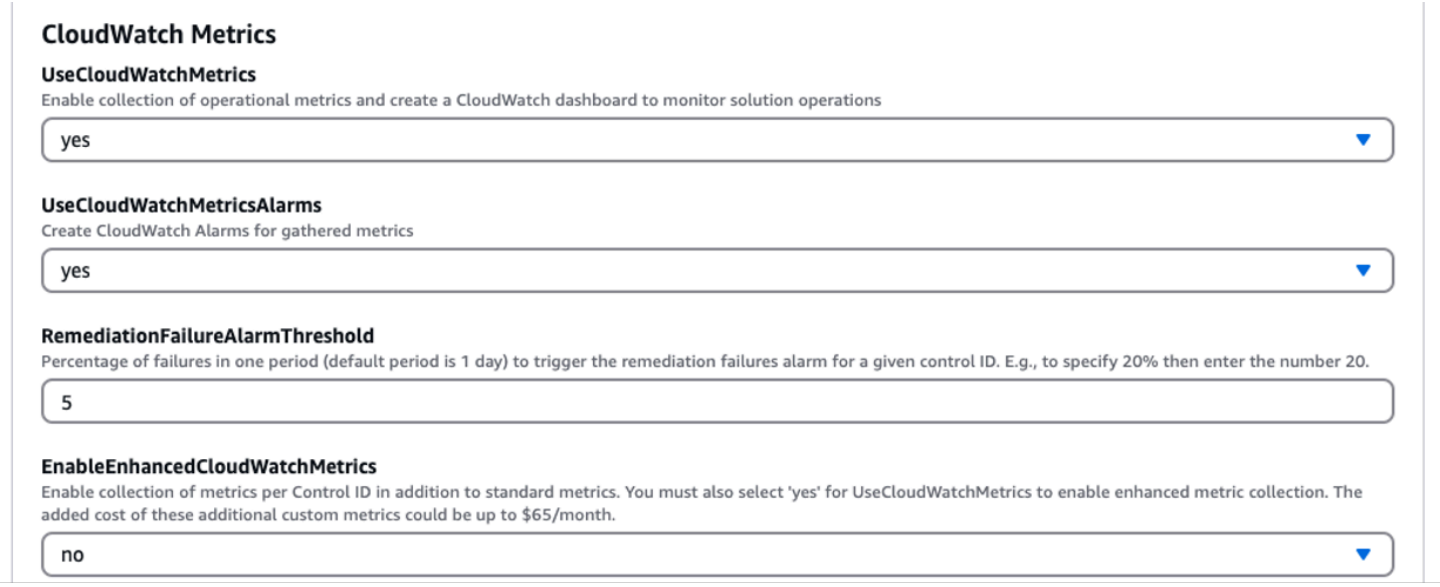
Überwachen Sie den Betrieb der Lösung mit einem CloudWatch Amazon-Dashboard

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

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

Aktivierung von CloudWatch Metriken, Alarmen und Dashboards

Es gibt vier CloudFormation Vorlagenparameter für die CloudWatch Funktionalität.



1. UseCloudWatchMetrics— Diese Einstellung `yes` ermöglicht die Erfassung von Betriebskennzahlen und erstellt ein CloudWatch Dashboard, in dem diese Kennzahlen angezeigt werden können.
2. UseCloudWatchAlarms- Wenn Sie diese Einstellung auf einstellen, werden die Standardalarme der Lösung `yes` aktiviert.
3. RemediationFailureAlarmThreshold- Der Prozentsatz fehlgeschlagener Problembehebungen in einem Zeitraum, in dem ein Alarm ausgelöst wurde.
4. EnableEnhancedCloudWatchMetrics- Stellen Sie diesen Parameter auf ein, `yes` um einzelne Metriken pro Kontroll-ID zu sammeln. Standardmäßig ist dieser Parameter auf gesetztno, sodass nur Metriken zur Gesamtzahl der Behebungen in allen Kontrollen erfasst IDs werden. Für einzelne Metriken und Alarme pro Kontroll-ID fallen zusätzliche Kosten an.

Verwenden des Dashboards CloudWatch

So zeigen Sie das Dashboard an:

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

Das Dashboard enthält die folgenden Abschnitte: CloudWatch

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

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

1. State Machine-Ausführungen > 1000 in einem Zeitraum von 24 Stunden.

   a. Ein starker Anstieg der Behebungsausführungen könnte darauf hindeuten, dass eine Ereignisregel häufiger als beabsichtigt initiiert wird.

   b. Der Schwellenwert kann mithilfe des Parameters geändert werden. CloudFormation

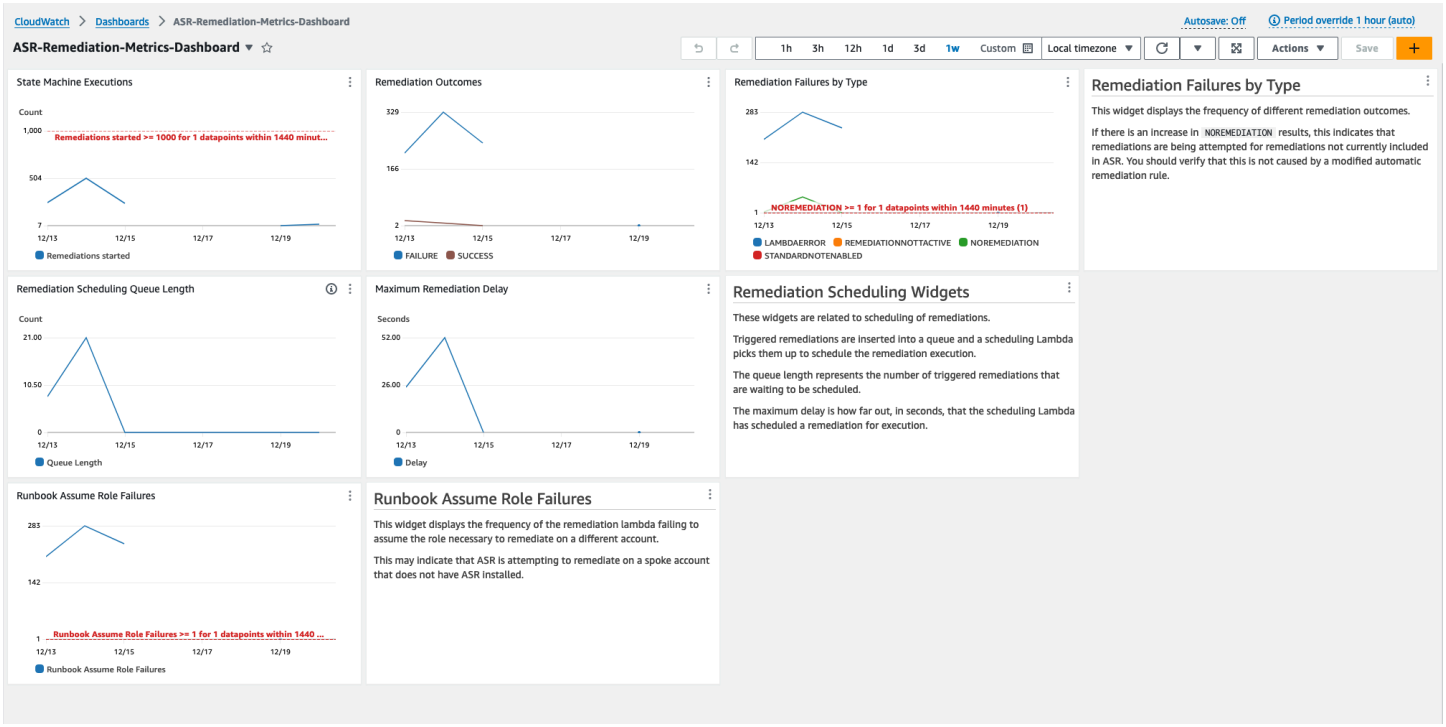
2. Behebungsfehler nach Typ = NOREMEDIATION > 0

   a. Für Behebungen, die nicht in ASR enthalten sind, werden Behebungsversuche unternommen. Dies könnte darauf hindeuten, dass eine Ereignisregel dahingehend geändert wurde, dass sie mehr als die vorgesehenen Behebungen umfasst.

3. Runbook Assume Role: Fehler > 0

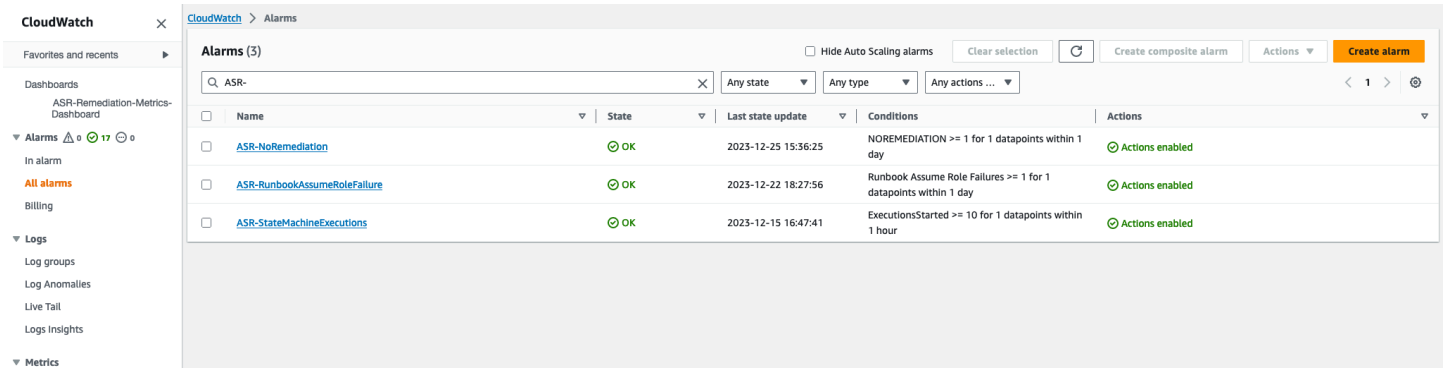
   a. Gegenmaßnahmen werden für Konten oder Regionen versucht, in denen die Lösung nicht ordnungsgemäß bereitgestellt wurde. Dies könnte darauf hindeuten, dass eine Ereignisregel dahingehend geändert wurde, dass sie mehr Konten als beabsichtigt umfasst.

Alle Alarmschwellenwerte können an die individuellen Einsatzanforderungen angepasst werden.

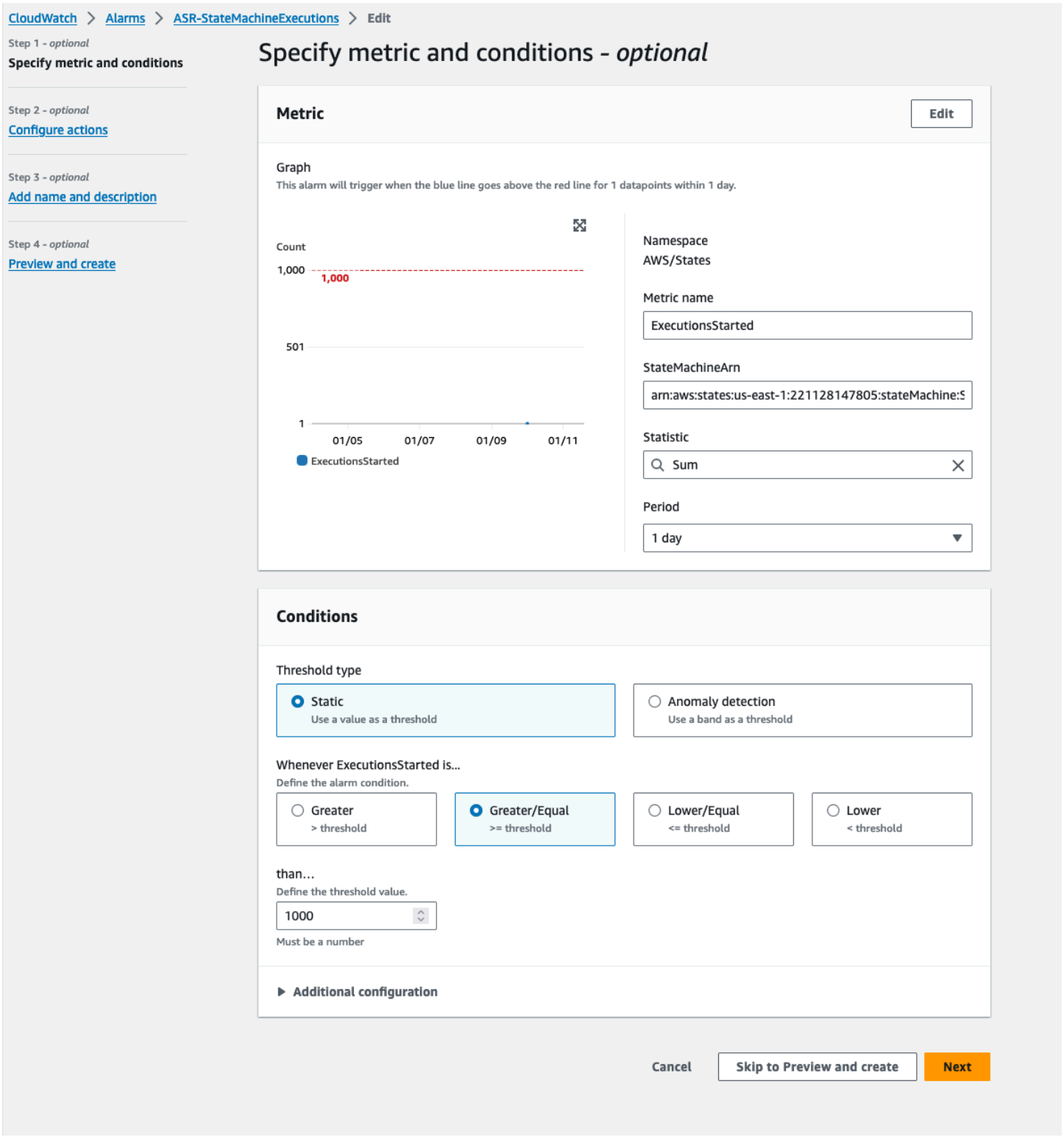


Änderung der Alarmschwellenwerte

1. Navigieren Sie zu Amazon CloudWatch → Alarme → Alle Alarme.
2. Wählen Sie den Alarm aus, den Sie ändern möchten, und wählen Sie dann Aktionen → Bearbeiten.



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

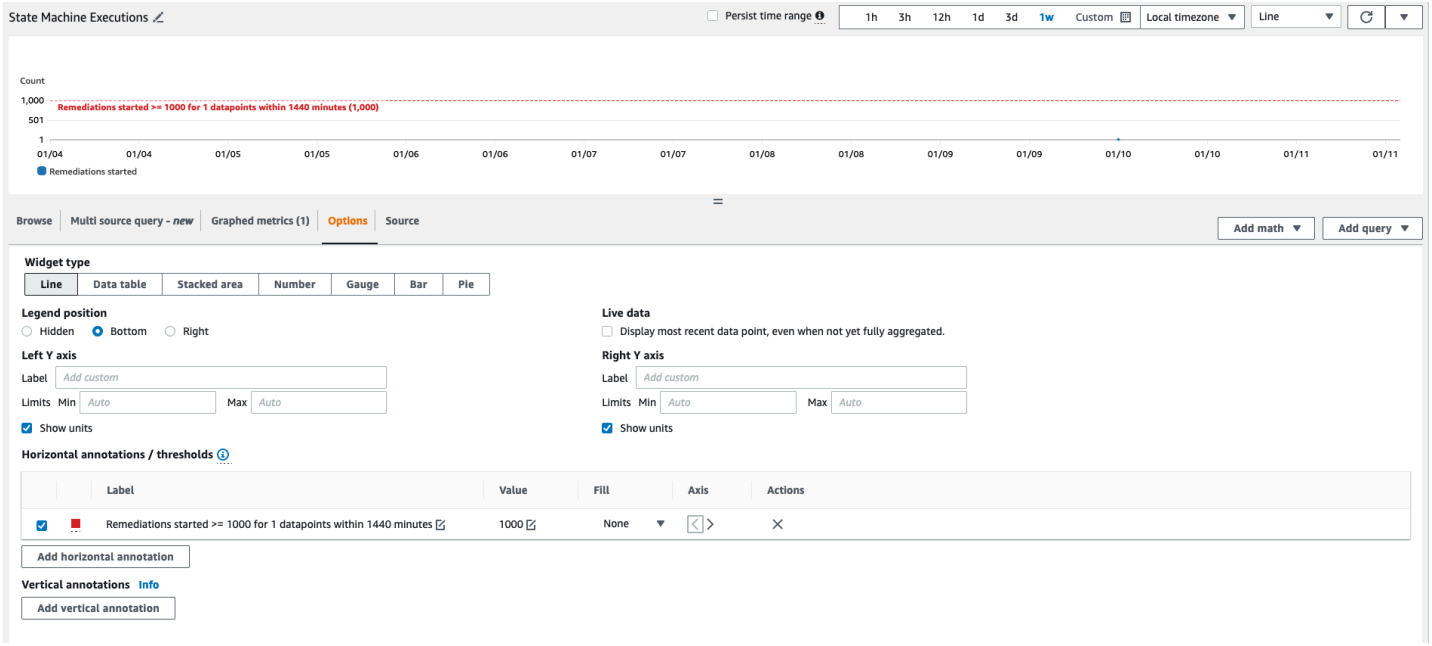


1. Navigieren Sie zum CloudWatch Dashboard, um die dortigen Diagramme an die neuen Einstellungen anzupassen.
   a. Wählen Sie die Ellipse oben rechts im entsprechenden Widget aus.

b. Wählen Sie Bearbeiten aus.

c. Wechseln Sie zur Registerkarte Optionen.

d. Passen Sie die Alarmanmerkung an die neuen Einstellungen an.



Alarmbenachrichtigungen abonnieren

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

Aktualisieren Sie die Lösung

Important

- Bei der Aktualisierung der Lösung müssen automatische Behebungsregeln möglicherweise manuell im Admin-Konto erneut aktiviert werden. Weitere Informationen finden Sie unter Vollautomatische Problembehebungen aktivieren.
- Wenn Sie den `Reuse Orchestrator Log Group` Parameter zur Aufbewahrung von Protokollen verwenden, stellen Sie sicher, dass er während der Stack-Aktualisierung richtig eingestellt ist, um eine Neuerstellung der Protokollgruppe oder den Verlust von Protokollaufbewahrungseinstellungen zu vermeiden. Weitere Informationen finden Sie unter Lösung bereitstellen. Wenn Sie ein Stack-Update auf v2.3.0+ von einer früheren Version durchführen, wählen Sie „Nein“

Upgrade von Versionen vor v1.4

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

1. Deinstallieren Sie die zuvor bereitgestellte Lösung. Weitere Informationen finden Sie unter Lösung deinstallieren.
2. Starten Sie die neueste Vorlage. Weitere Informationen finden Sie unter Bereitstellen der Lösung.

Note

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

Aktualisierung von Version 1.4 und höher

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

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

Upgrade von v2.0.x

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

Ein Upgrade von Version 2.1.4 oder früher

Wenn Sie ein Upgrade von v2.1.4 oder früher durchführen, müssen Sie ein Upgrade auf v2.3.0 durchführen, bevor Sie auf eine höhere Version als v2.3.0 aktualisieren. Andernfalls schlägt der Stack-Aktualisierungsvorgang fehl. Alternativ können Sie die Stacks der Lösung löschen und erneut bereitstellen, anstatt ein Stack-Update durchzuführen.

Fehlerbehebung

Die Lösung bekannter Probleme enthält Anweisungen zur Behebung bekannter Fehler. Wenn diese Anweisungen Ihr Problem nicht lösen, finden Sie unter Wenden Sie sich an den AWS-Support. Dort finden Sie Anweisungen zum Öffnen einer AWS-Supportanfrage für diese Lösung.

Lösungsprotokolle

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

Diese Lösung sammelt die Ausgabe von Remediation-Runbooks, die unter AWS Systems Manager ausgeführt werden, und protokolliert das Ergebnis in der Gruppe CloudWatch Logs `SO0111-ASR` im AWS Security Hub-Administratorkonto. Es gibt einen Stream pro Kontrolle und Tag.

Die Orchestrator Step Functions protokollieren alle Schrittübergänge in der `SO0111-ASR-Orchestrator` CloudWatch Logs-Gruppe im AWS Security Hub-Administratorkonto. Dieses Protokoll ist ein Audit-Trail, um Zustandsübergänge für jede Instanz der Step Functions aufzuzeichnen. Pro Ausführung von Step Functions gibt es einen Protokollstream.

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

Die folgenden Informationen zur Fehlerbehebung verwenden die `SO0111-ASR` Protokollgruppe. Verwenden Sie dieses Protokoll sowie die AWS Systems Manager Automation-Konsole, Automation Executions-Protokolle, Step Function-Konsole und Lambda-Protokolle, um Probleme zu beheben.

Schlägt eine Problembehebung fehl, wird eine Meldung ähnlich der folgenden `SO0111-ASR` im Log-Stream für Standard, Kontrolle und Datum protokolliert. Zum Beispiel: CIS-2.9-2021-08-12

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

Die folgenden Meldungen enthalten zusätzliche Informationen. Diese Ausgabe stammt aus dem ASR-Runbook für den Sicherheitsstandard und die Sicherheitssteuerung. Zum Beispiel: ASR-CIS_1.2.0_2.9

```
Step fails when it is Execution complete: verified. Failed to run automation with
 executionId: eecdef79-9111-4532-921a-e098549f5259 Failed :
```

```
{Status=[Failed], Output=[No output available yet because the step is not successfully
 executed], ExecutionId=[eecdef79-9111-4532-921a-e098549f5259]}. Please refer to
 Automation Service Troubleshooting Guide for more diagnosis details.
```

Diese Informationen weisen Sie auf den Fehler hin, bei dem es sich in diesem Fall um eine untergeordnete Automatisierung handelte, die im Mitgliedskonto ausgeführt wurde. Um dieses Problem zu beheben, müssen Sie sich im Mitgliedskonto (aus der obigen Nachricht) bei der AWS-Managementkonsole anmelden, zu AWS Systems Manager wechseln, zu Automation navigieren und die Protokollausgabe auf Execution ID überprüfen`eecdef79-9111-4532-921a-e098549f525`.

Lösung eines bekannten Problems

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

  Lösung: Suchen Sie im Abschnitt „ CloudFormation Ressourcen/Ereignisse“ nach einer Fehlermeldung, die darauf hinweist, dass Protokollgruppen bereits existieren. Die ASR-Bereitstellungsvorlagen ermöglichen die Wiederverwendung vorhandener Protokollgruppen. Stellen Sie sicher, dass Sie die Wiederverwendung ausgewählt haben.
- Problem: Die Bereitstellung der Lösung schlägt fehl und es wird ein Fehler in einem verschachtelten Playbook-Stapel angezeigt, in dem eine EventBridge Regel nicht erstellt werden kann

  Lösung: Sie haben wahrscheinlich das Kontingent für EventBridge Regeln mit der Anzahl der bereitgestellten Playbooks erreicht. Sie können dies vermeiden, indem Sie die konsolidierten Kontrollergebnisse in Security Hub zusammen mit dem SC-Playbook in dieser Lösung verwenden, nur die Playbooks für die verwendeten Standards bereitstellen oder eine Erhöhung des EventBridge Regelkontingents beantragen.
- Problem: Ich betreibe Security Hub in mehreren Regionen mit demselben Konto. Ich möchte diese Lösung in mehreren Regionen einsetzen.

  Lösung: Stellen Sie den Admin-Stack im selben Konto und in derselben Region bereit wie Ihr Security Hub-Administrator. Installieren Sie die Mitgliedsvorlage in jedem Konto und jeder Region, in der Sie ein Security Hub Hub-Mitglied konfiguriert haben. Aktivieren Sie die Aggregation im Security Hub.
- Problem: Unmittelbar nach der Bereitstellung schlägt der SO0111-ASR-Orchestrator im Status Get Automation Document mit einem 502-Fehler fehl: „`Lambda konnte die Umgebungsvariablen

nicht entschlüsseln, weil der KMS-Zugriff verweigert wurde. Bitte überprüfen Sie die KMS-Schlüsseleinstellungen der Funktion. KMS-Ausnahme: UnrecognizedClientException KMS-Nachricht: Das in der Anfrage enthaltene Sicherheitstoken ist ungültig. (Dienst: AWSLambda; Statuscode: 502; Fehlercode: KMSAccessDeniedException; Anforderungs-ID:... `"

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

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

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

  Lösung: Die Security Hub Hub-Konsole wird nicht automatisch aktualisiert. Aktualisieren Sie die aktuelle Ansicht. Der Status des Ergebnisses sollte aktualisiert werden. Es kann mehrere Stunden dauern, bis das Ergebnis von „Fehlgeschlagen“ auf „Bestanden“ umgestellt wird. Die Ergebnisse werden anhand von Ereignisdaten erstellt, die von anderen Services wie AWS Config an AWS Security Hub gesendet werden. Die Zeit, bis eine Regel neu bewertet wird, hängt vom zugrunde liegenden Service ab. Falls das Problem dadurch nicht behoben wird, finden Sie weitere Informationen in der vorherigen Lösung unter „`Ich habe versucht, ein Ergebnis zu korrigieren, aber es ist nichts passiert. `“
- Problem: Die Orchestrator-Schrittfunktion schlägt in Get Automation Document State fehl: Beim Aufrufen des AssumeRole Vorgangs ist ein Fehler aufgetreten (AccessDenied).

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

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

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

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

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

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

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

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

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

  a. Melden Sie sich bei der AWS Security Hub-Managementkonsole an.

  b. Gehen Sie im Admin-Konto zu Einstellungen.

  c. Wählen Sie den Tab Benutzerdefinierte Aktionen

  d. Löschen Sie den Eintrag Remediate with ASR manuell.

  e. Löschen Sie den Stapel erneut.

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

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

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

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

  Lösung: Dies kommt häufig vor, wenn Sie im Mitgliedskonto keine Abonnements für das `SO0111-ASR_LocalAlarmNotification` SNS-Thema haben.

Probleme mit bestimmten Abhilfemaßnahmen

Set SSLBucket Policy schlägt mit einem AccessDenied Fehler fehl

Dazugehörige Steuerungen: AWS FSBP v1.0.0 S3.5, PCI v3.2.1 PCI.S3.5, CIS v1.4.0 2.1.2, SC v2.0.0 S3.5

ProblemSSLBucket: Die Option „ AccessDenied Richtlinie festlegen“ schlägt mit einem Fehler fehl:

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

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

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

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

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

PutS3 schlägt fehl BucketPolicyDeny

Dazugehörige Steuerungen: AWS FSBP v1.0.0 S3.6, NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2

ProblemBucketPolicyDeny : Der PutS3 mit dem folgenden Fehler:

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

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

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

Wie deaktiviere ich die Lösung

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

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

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

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

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

Szenario 3: Deaktivieren Sie die manuelle Problembehebung für ein Konto

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

Support kontaktieren.

Wenn Sie über AWS Developer Support, AWS Business Support oder AWS Enterprise Support verfügen, können Sie das Support Center nutzen, um fachkundige Unterstützung zu dieser Lösung zu erhalten. In den folgenden Abschnitten finden Sie entsprechende Anweisungen.

Fall erstellen

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

Wie können wir helfen?

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

Zusätzliche Informationen

1. Geben Sie als Betreff einen Text ein, der Ihre Frage oder Ihr Problem zusammenfasst.
2. Beschreiben Sie das Problem im Feld Beschreibung detailliert.

3. Wählen Sie Dateien anhängen.
4. Fügen Sie die Informationen bei, die der Support zur Bearbeitung der Anfrage benötigt.

Helfen Sie uns, Ihren Fall schneller zu lösen

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

Löse es jetzt oder kontaktiere uns

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

Deinstalliere die Lösung

Gehen Sie wie folgt vor, um die Lösung mit der AWS-Managementkonsole zu deinstallieren.

V1.0.0-V1.2.1

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

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

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

V1.3.x

1. Entfernen Sie das `automated-security-response-member.template` von jedem Mitgliedskonto.
2. Entfernen Sie das `automated-security-response-admin.template` aus dem Administratorkonto.

> **Note**
>
> Das Entfernen der Admin-Vorlage in Version 1.3.0 schlägt wahrscheinlich fehl, wenn die benutzerdefinierte Aktion entfernt wird. Dies ist ein bekanntes Problem, das in der nächsten Version behoben wird. Verwenden Sie die folgenden Anweisungen, um dieses Problem zu beheben:
>
> 1. Melden Sie sich bei der AWS Security Hub-Managementkonsole an.
> 2. Gehen Sie im Administratorkonto zu Einstellungen.
> 3. Wählen Sie den Tab Benutzerdefinierte Aktionen aus.
> 4. Löschen Sie den Eintrag Remediate with ASR manuell.
> 5. Löschen Sie den Stapel erneut.

V1.4.0 und höher

Stack-Bereitstellung

1. Entfernen Sie das `automated-security-response-member.template` aus jedem Mitgliedskonto.
2. Entfernen Sie das `automated-security-response-admin.template` aus dem Administratorkonto.

StackSet Bereitstellung

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

Beachten Sie, dass IAM-Rollen aus dem beibehalten `automated-security-response-member-roles.template` werden, auch wenn die Vorlage entfernt wird. Auf diese Weise können Behebungen, die diese Rollen verwenden, weiterhin funktionieren. Diese SO0111-*-Rollen können manuell entfernt werden, nachdem sichergestellt wurde, dass sie nicht mehr verwendet werden, und zwar durch aktive Behebungsmaßnahmen, z. B. CloudTrail für die Protokollierung oder RDS Enhanced Monitoring. CloudWatch

Administratorhandbuch

Teile der Lösung aktivieren und deaktivieren

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

Wo die Stacks für Mitglieder und Mitgliederrollen bereitgestellt werden:

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

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

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

Welche verschachtelten Standard-Stacks werden bereitgestellt:

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

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

Welche Control-Runbooks werden in jedem verschachtelten Mitglieds-Stack bereitgestellt:

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

SSM-Parameter für die Aktivierung und Deaktivierung von Standards:

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

Zugriff auf die Weboberfläche der Lösung:

- Wenn der Admin-Stack bereitgestellt ist, erhalten Sie eine E-Mail mit temporären Anmeldeinformationen, mit denen Sie sich mit der E-Mail-Adresse, die Sie bei der Bereitstellung angegeben haben, auf der Webbenutzeroberfläche anmelden können.
- Auf der Seite „Benutzer einladen“ können Administratoren und delegierte Administratoren weitere Benutzer zum Zugriff auf die Web-Benutzeroberfläche einladen und den Zugriff auf die Lösung delegieren.
- Auf der Seite „Benutzer anzeigen“ können Administratoren und delegierte Administratoren bestehende Benutzer anzeigen und verwalten.
- Weitere Informationen zu Berechtigungen und zur Verwendung der Web-Benutzeroberfläche der Lösung finden Sie im Web UI Developer Guide.

Beispiel für SNS-Benachrichtigungen

Wenn eine Problembehebung eingeleitet wird

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

Wenn eine Sanierung erfolgreich ist

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

```
}
```

Wenn eine Korrektur fehlschlägt

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

Tutorial

Dies ist ein Tutorial, das Sie durch Ihren ersten Einsatz von ASR führt. Es beginnt mit den Voraussetzungen für die Bereitstellung der Lösung und endet damit, dass Sie Beispielprobleme in einem Mitgliedskonto korrigieren.

Tutorial: Erste Schritte mit Automated Security Response auf AWS

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

Bereiten Sie die Konten vor

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

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

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

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
`111111111111`	Admin.	Keine	Keine
`222222222222`	Mitglied	Keine	Keine

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

jedoch nicht das Administratorkonto von AWS Organizations für die AWS-Organisation sein, zu der Ihre Konten gehören.

AWS Config aktivieren

Lesen Sie die folgende Dokumentation:

- Dokumentation zu AWS Config
- Preise für AWS Config
- AWS Config aktivieren

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

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

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

AWS-Sicherheitshub aktivieren

Lesen Sie die folgende Dokumentation:

- Dokumentation zu AWS Security Hub
- Preise für AWS Security Hub
- AWS Security Hub aktivieren

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

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

Ermöglichen Sie konsolidierte Kontrollergebnisse

Lesen Sie die folgende Dokumentation:

- Generierung und Aktualisierung der Kontrollergebnisse

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

Ermöglichen Sie konsolidierte Kontrollergebnisse für beide Konten und beide Regionen.

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

Es kann einige Zeit dauern, bis die Ergebnisse mit der neuen Funktion generiert werden. Sie können mit dem Tutorial fortfahren, aber Sie können die ohne die neue Funktion generierten Ergebnisse

nicht korrigieren. Mit der neuen Funktion generierte Ergebnisse können anhand des `GeneratorId` Feldwerts `security-control/<control_id>` identifiziert werden.

Konfigurieren Sie die regionsübergreifende Suchaggregation

Lesen Sie die folgende Dokumentation:

- Regionsübergreifende Aggregation
- Aktivierung der regionsübergreifenden Aggregation

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

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Konfigurieren Sie die Aggregation von us-west-2	Keine
222222222222	Mitglied	Aggregation von us-west-2 aus konfigurieren	Keine

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

Benennen Sie ein Security Hub-Administratorkonto

Lesen Sie die folgende Dokumentation:

- Verwaltung von Konten in AWS Security Hub
- Verwaltung der Mitgliedskonten von Organisationen
- Verwaltung von Mitgliedskonten auf Einladung

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

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

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Laden Sie das Mitgliedskonto ein	Keine
222222222222	Mitglied	Nehmen Sie die Einladung an	Keine

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

Erstellen Sie die Rollen für selbstverwaltete Berechtigungen StackSets

Lesen Sie die folgende Dokumentation:

- AWS CloudFormation StackSets
- Gewähren Sie selbstverwaltete Berechtigungen

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

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

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Stellen Sie den StackSet Administr	Keine

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
		ator-Rollenstapel bereit Stellen Sie den StackSet Ausführun gs-Rollenstapel bereit	
222222222222	Mitglied	Stellen Sie den StackSet Ausführun gsrollen-Stack bereit	Keine

Erstellen Sie die unsicheren Ressourcen, die zu Beispielergebnissen führen

Lesen Sie die folgende Dokumentation:

- Referenz zu Security Hub-Steuerungen
- AWS Lambda Lambda-Steuerungen

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

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

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

Berechtigungen eine Richtlinienerklärung hinzu, um das Aufrufen der Funktion über die URL ohne Authentifizierung zu ermöglichen.

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

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Keine	Keine
222222222222	Mitglied	Keine	Erstellen Sie eine Lambda-Funktion mit einer unsicheren Konfiguration

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

Erstellen Sie CloudWatch Protokollgruppen für verwandte Steuerelemente

Lesen Sie die folgende Dokumentation:

- Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs
- CloudTrail Kontrollen

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

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

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

Stellen Sie die Lösung für Tutorial-Konten bereit

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

Stellen Sie den Admin-Stack bereit

View template

automa

security-response-admin.vorlage

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

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

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

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Stellen Sie den Admin-Stack bereit	Keine
222222222222	Mitglied	Keine	Keine

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

Stellen Sie den Mitglieds-Stack bereit

View template

automa

security-response-member.vorlage

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

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

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

Geben Sie die ID des Administratorkontos als Wert für den Parameter für die Admin-Kontonummer ein. In unserem Beispiel ist das111111111111.

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

Stellen Sie den Mitgliederrollen-Stack bereit

automated-security-response-member-roles.template-Vorlagenschaltfläche -roles.template automated-security-response-member

Navigieren Sie im Administratorkonto zur CloudFormation StackSets Konsole und stellen Sie den Mitgliederstapel für jedes Konto bereit. Verwenden Sie die in diesem Tutorial erstellten StackSets Admin- und Ausführungsrollen. Geben Sie die ID des Administratorkontos als Wert für den Parameter für die Admin-Kontonummer ein. In unserem Beispiel ist das111111111111.

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

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

Abonnieren Sie das SNS-Thema

Aktualisierungen zur Problembehebung

Thema - {https---us-east-1-console-aws-amazon-com-sns-v3- home-region-us-east -1— topic-arn-aws-sns -US-East-1-221128147805-SO0111-ASR-Topic} [SO0111-ASR_Topic]

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

Alarme

Thema - {https---us-east-1-console-aws-amazon-com-sns-v3- home-region-us-east -1— topic-arn-aws-sns -US-East-1-221128147805-SO0111-ASR-Alarm-Topic} [SO0111-ASR_Alarm_Topic]

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

Korrigieren Sie die Ergebnisse der Beispiele

> **Important**
>
> Dieses Beispiel erfordert die Verwendung der Security Hub CSPM-Konsole. Die Security Hub Hub-Konsole (ohne CSPM) unterstützt derzeit keine manuellen Problembehebungen durch benutzerdefinierte Aktionen. Informationen zur Behebung von Ergebnissen ohne Verwendung der Security Hub CSPM-Konsole finden Sie im Abschnitt Korrigieren mithilfe der Web-UI.

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

Dies kann auf verschiedene Arten geschehen:

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

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

Initiieren Sie die Behebung

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

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Initiieren Sie die Sanierung	Keine
222222222222	Mitglied	Keine	Keine

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

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

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Keine	Keine
222222222222	Mitglied	Keine	Vergewissern Sie sich, dass die Behebung erfolgreich war

Korrigieren Sie mithilfe der Webbenutzeroberfläche

Alternativ können Sie die Weboberfläche der Lösung verwenden, um die Ergebnisse von AWS Security Hub zu korrigieren und frühere Abhilfemaßnahmen einzusehen.

> **Note**
>
> Sie müssen den `ShouldDeployWebUI` Parameter bei der Bereitstellung des Admin-Stacks auf „yes“ setzen, um die Web-UI der Lösung verwenden zu können.

Melden Sie sich bei der Web-UI an

Nach der Bereitstellung der Lösung erhalten Sie von no-reply@verificationemail.com eine E-Mail mit temporären Anmeldeinformationen und einem Link zur Weboberfläche der Lösung. Dies wird an die E-Mail-Adresse gesendet, die Sie bei der Bereitstellung des Admin-Stacks angegeben haben.

Suchen Sie die E-Mail, kopieren Sie die temporären Anmeldeinformationen und klicken Sie auf den Link zur Web-Benutzeroberfläche. Über diesen Link gelangen Sie direkt zur Anmeldeseite, auf der Sie Ihre temporären Anmeldeinformationen eingeben und ein neues Passwort festlegen können.

Suchen Sie den Lambda.1-Befund

Sobald Sie sich angemeldet haben, wird Ihnen die Seite mit den Ergebnissen angezeigt. Auf dieser Seite werden alle Security Hub-Ergebnisse in Ihrem Security Hub-Administratorkonto angezeigt, deren Behebung unterstützt wird, einschließlich der Ergebnisse für Mitgliedskonten, die bei AWS Security Hub integriert sind.

Verwenden Sie auf der Seite Ergebnisse die Suchleiste, um nach der Ressourcen-ID zu filtern, indem Sie den ARN der Lambda-Funktion eingeben, die Sie im Rahmen dieses Tutorials erstellt haben, und eine Suche mit dem Operator „=“ durchführen. Daraufhin werden alle Ergebnisse von AWS Security Hub angezeigt, die von der Lösung für die von Ihnen erstellte Lambda-Funktion unterstützt wurden.

Um das in diesem Tutorial generierte `Lambda.1` Ergebnis zu finden, wenden Sie einen weiteren Filter auf Finding Type an. Klicken Sie auf die Suchleiste, wählen Sie Finding Type und dann den Operator „=“ aus. Wenn Consolidated Control Findings in Ihrer Umgebung aktiviert ist, geben Sie ein`security-control/Lambda.1`. Wählen Sie andernfalls einen Sicherheitsstandard, der das Lambda.1-Steuerelement unterstützt, und geben Sie beispielsweise die Generator-ID ein. `aws-foundational-security-best-practices/v/1.0.0/Lambda.1`

Nachdem Sie die Filter Ressourcen-ID und Finding Type angewendet haben, sehen Sie in der Tabelle nur das Lambda.1-Ergebnis, das von AWS Security Hub für Ihre Testressource generiert wurde.

> **Note**
>
> Es kann einige Zeit dauern, bis AWS Security Hub den Lambda.1-Befund für die von Ihnen erstellte Ressource generiert hat. Wenn Sie das Ergebnis nicht sehen, nachdem Sie beide Filter angewendet haben, warten Sie 5-10 Minuten und suchen Sie erneut nach dem Ergebnis.

Initiieren Sie die Behebung

Wählen Sie das Ergebnis aus, das Sie im vorherigen Schritt gefunden haben, und klicken Sie dann auf Aktionen > Korrigieren. Dadurch wird mit der Behebung des von Ihnen ausgewählten Befundes begonnen.

Sie können den Fortschritt dieser Behebung auf der Seite Ausführungsverlauf einsehen. Nachdem Sie einige Minuten gewartet haben, aktualisieren Sie die Seite mit dem Ausführungsverlauf, indem Sie oben rechts auf das Aktualisierungssymbol klicken. Sie sollten dann sehen, dass sich der Status von `In progress` zu `Success` geändert hat.

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

Wenn das Ergebnis als `Resolved` von AWS Security Hub gekennzeichnet ist, wird es automatisch von der Findings-Seite in der Web-UI entfernt.

Um zu überprüfen, ob das Problem durch die Behebung behoben wurde, navigieren Sie im Mitgliedskonto zur Lambda-Konsole und bestätigen Sie, dass der öffentliche Zugriff gesperrt wurde.

> **Note**
>
> Einige Ergebnisse werden möglicherweise auch dann noch auf der Seite „Ergebnisse“ angezeigt, wenn der Behebungsstatus lautet. `Success` Dies liegt daran, dass AWS Security Hub bis zu 24 Stunden benötigt, um ein Problem nach der Aktualisierung der Ressource als behoben zu kennzeichnen. Sie können Ergebnisse, die Sie nicht mehr auf der Ergebnisseite sehen möchten, unterdrücken, indem Sie das Ergebnis auswählen und auf Aktionen > Unterdrücken klicken.

Verfolgen Sie die Ausführung der Problembehebung

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

EventBridge Regel

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

Ausführung von Step Functions

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

SSM-Automatisierung

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

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

CloudWatch Gruppe protokollieren

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

Ermöglichen Sie vollautomatische Problembehebungen

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

> **Important**
>
> Bevor Sie vollautomatische Problembehebungen aktivieren, stellen Sie sicher, dass die Lösung in den Konten und Regionen konfiguriert ist, in denen Sie den Anforderungen

entsprechen, dass die Lösung automatische Änderungen vornimmt. Wenn Sie den Umfang der automatisierten Problembehebungen der Lösung einschränken möchten, lesen Sie den nachfolgenden Abschnitt über das Filtern vollautomatischer Abhilfemaßnahmen.

Beispiel: Vollautomatische Problembehebungen für Lambda.1 aktivieren

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

Important

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

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

Suchen Sie die DynamoDB-Tabelle für die Behebungskonfiguration.

Sehen Sie sich im Administratorkonto den Stack `Outputs` für den Admin-Stack in der Konsole an. CloudFormation Sie sehen eine Ausgabe mit dem Titel`RemediationConfigurationDynamoDBTable`.

Dies ist der Name der DynamoDB-Tabelle „Remediation Configuration“, die automatisierte Behebungskonfigurationen für die Lösung steuert. Kopieren Sie den Wert dieser Ausgabe und suchen Sie die entsprechende DynamoDB-Tabelle in der DynamoDB-Konsole.

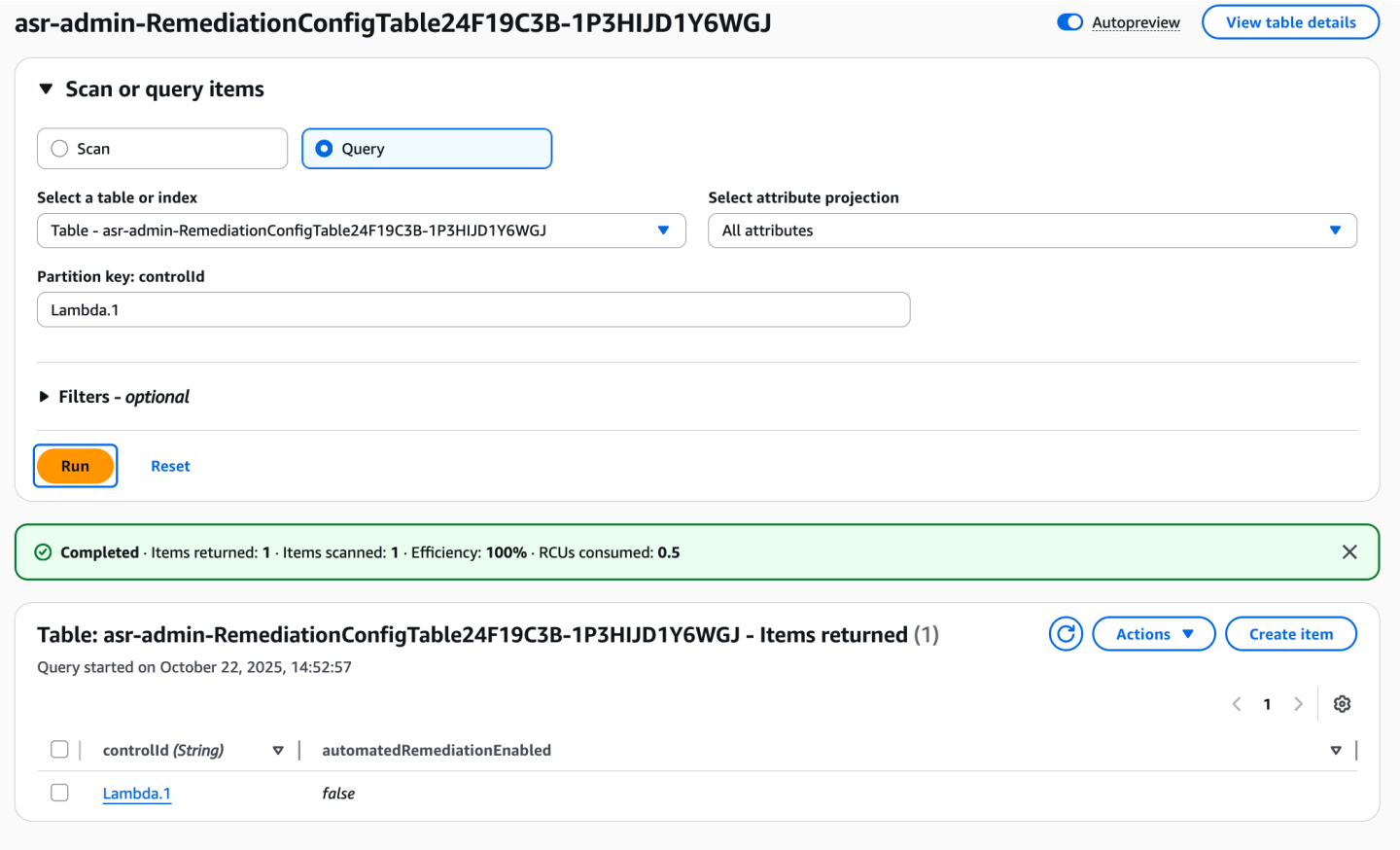
Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Suchen Sie die DynamoDB-Tabelle „Remediation Configuration“.	Keine
222222222222	Mitglied	Keine	Keine

Ändern Sie die Tabelle mit der Behebungskonfiguration

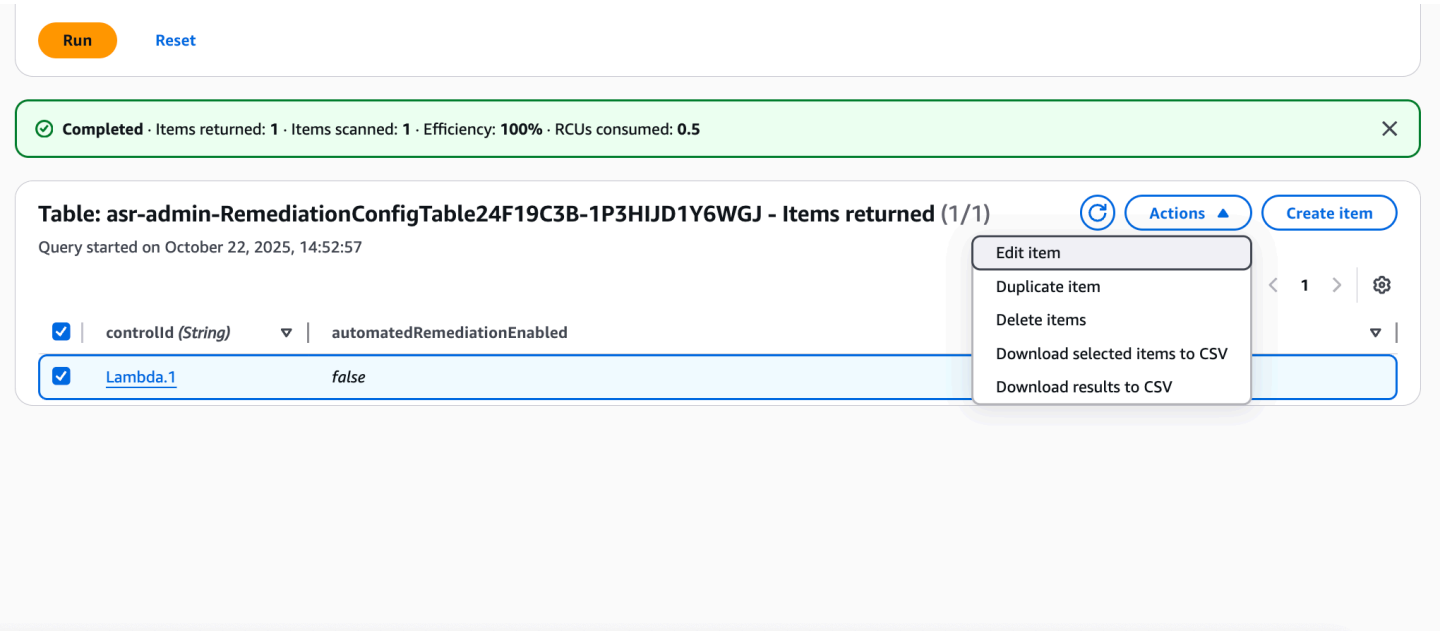
Wählen Sie in der DynamoDB-Konsole, in der Sie die Tabelle mit der Behebungskonfiguration gefunden haben, die Option Tabellenelemente durchsuchen aus.

Jedes Element in der Tabelle entspricht einem Security Hub-Steuerelement, das von der Lösung unterstützt wird. Jedes Element hat ein `automatedRemediationEnabled` Attribut, das geändert werden kann, um vollautomatische Korrekturen für das zugehörige Steuerelement zu ermöglichen.

Um Lambda.1 zu aktivieren, wählen Sie unter Elemente scannen oder abfragen die Option Abfrage aus. Geben Sie unter Partitionsschlüssel: ControlID die Eingabe ein **`Lambda.1`** und klicken Sie auf Ausführen. Es wird ein einziger Artikel zurückgegeben, der der Lambda.1-Steuerung entspricht.



Wählen Sie nun das `Lambda.1` Element aus und klicken Sie dann auf Aktionen > Element bearbeiten.



Ändern Sie abschließend den `automatedRemediationEnabled` Attributwert in True. Klicken Sie auf Speichern und schließen.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Ändern Sie die DynamoDB-Tabelle für die Behebungs konfiguration.	Keine
222222222222	Mitglied	Keine	Keine

Konfigurieren Sie die Ressource

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

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Keine	Keine
222222222222	Mitglied	Keine	Konfigurieren Sie die Lambda-Funktion, um öffentlichen Zugriff zu ermöglichen

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

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

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Keine	Keine
222222222222	Mitglied	Keine	Vergewissern Sie sich, dass die Behebung erfolgreich war

(Optional) Konfigurieren Sie die Filterung für vollautomatische Problembehebungen

Wenn Sie den Umfang einschränken möchten, in dem die Lösung Behebungen ausführt, können Sie Filter anwenden. Diese Filter gelten nur für vollautomatische Behebungen und wirken sich nicht auf manuell aufgerufene Behebungen aus.

Die Lösung bietet Filterung nach den folgenden Dimensionen:

1. Konto-IDs
2. Organisationseinheiten (OUs)
3. Ressourcen-Tags

Jede Dimension ist konfigurierbar, indem die von der Lösung bereitgestellten Systems Manager Manager-Parameter entsprechend der angegebenen Dimension geändert werden. Alle Filterparameter im Parameter Store befinden sich im Admin-Konto unter dem `/ASR/Filters/` Pfad.

Jede Dimension hat zwei Parameter für die Konfiguration, einen für den Filterwert und einen weiteren für den Filtermodus. Die Dimension Account-IDs hat beispielsweise zwei Parameter mit dem Namen `/ASR/Filters/AccountFilters` und`/ASR/Filters/AccountFilterMode`. Beide müssen geändert werden, um die Filterung nach Konto-IDs zu konfigurieren.

Um beispielsweise vollautomatische Problembehebungen darauf zu beschränken, nur für Konten 111111111111 und Konten ausgeführt zu werden, würden Sie den Wert von auf „111111111111**222222222222**, **`/ASR/Filters/AccountFilters`** 2222222222222222" ändern. Ändern Sie dann den Wert von in „Include“. `/ASR/Filters/AccountFilterMode` Die Lösung ignoriert dann alle Ergebnisse, die für andere Konten als 111111111111 oder 222222222222 generiert wurden.

Jeder Filterparameter benötigt eine kommagetrennte Werteliste, nach der gefiltert werden soll, und jeder „Modus“ -Parameter kann entweder auf Include, Exclude oder Disabled gesetzt werden.

Bereinigen

Löschen Sie die Beispielressourcen

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

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Keine	Keine
222222222222	Mitglied	Keine	Löschen Sie die Lambda-Beispielfunktion

Löschen Sie den Admin-Stack

Löschen Sie im Admin-Konto den Admin-Stack.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Löschen Sie den Admin-Stack	Keine
222222222222	Mitglied	Keine	Keine

Löschen Sie den Mitgliederstapel

Löschen Sie das Mitglied im Admin-Konto StackSet.

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

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
		Bestätigen Sie, dass die Mitgliederliste gelöscht	
222222222222	Mitglied	Bestätigen Sie, dass der Mitgliederstapel	Bestätigen Sie, dass der Mitgliederstapel

Löschen Sie den Stapel der Mitgliedsrollen

Löschen Sie im Admin-Konto die Mitgliedsrollen StackSet.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Löschen Sie die Mitgliederrollen StackSet Bestätigen Sie, dass der Rollenstapel gelöscht wurde	Keine
222222222222	Mitglied	Bestätigen Sie, dass der Rollenstapel für Mitglieder	Keine

Löschen Sie die beibehaltenen Rollen

Löschen Sie in jedem Konto die beibehaltenen IAM-Rollen.

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

Löschen Sie alle Rollen mit dem Präfix SO0111 -.

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Beibehaltene Rollen löschen	Keine
222222222222	Mitglied	Beibehaltene Rollen löschen	Keine

Planen Sie das Löschen der gespeicherten KMS-Schlüssel ein

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

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

Identifizieren Sie die von der Lösung bereitgestellten Schlüssel anhand der von der Lösung erstellten Aliase oder anhand des CloudFormation Verlaufs. Planen Sie, dass sie gelöscht werden.

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

Löschen Sie die Stacks für selbstverwaltete Berechtigungen StackSets

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

Account	Zweck	Aktion in US-East-1	Aktion in US-West-2
111111111111	Admin.	Löschen Sie den StackSet Administrator-Rollenstapel	Keine
222222222222	Mitglied	Löschen Sie den StackSet Ausführungsrollenstapel	Keine

Leitfaden für Entwickler

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

Quellcode

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

Spielbücher

Diese Lösung umfasst die Playbook-Korrekturen für die Sicherheitsstandards, die im Rahmen des Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmarkv3.0.0, AWS FoundationalSecurity Best Practices (FSBP) v.1.0.0, Payment Card Industry Data Security Standard (PCI-DSS)v3.2.1 und National Institute of Standards and Technology (NIST) definiert wurden.

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

> **Important**
>
> Stellen Sie die Playbooks nur für die aktivierten Standards bereit, um zu vermeiden, dass Servicekontingenten erreicht werden.

Einzelheiten zu einer bestimmten Problembehebung finden Sie im Systems Manager Manager-Automatisierungsdokument mit dem Namen, der von der Lösung in Ihrem Konto bereitgestellt wird. Gehen Sie zur AWS Systems Manager Manager-Konsole und wählen Sie dann im Navigationsbereich Dokumente aus.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
Vollständige Abhilfemaßnahmen	63	34	29	33	65	19	90
ASR-Prüfen EnableAutoScalingGroup ELBHealth Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten Load Balancer-Zustandsprüfungen verwenden	Autoscaling.1		Automatische Skalierung.1		Automatische Skalierung.1		Automatische Skalierung.1
ASR-Configure AutoScali					Autoscaling.3		Automatisches

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ngLaunchConfigToRequire IMDSv2 Auto Scaling Scaling-Gruppenstartkonfigurationen sollten EC2 Instances so konfigurieren, dass sie Instance Metadata Service Version 2 (IMDSv2) benötigen							Skalieren.3

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-CreateCloudTrailMultiRegionTrail CloudTrail sollte aktiviert und mit mindestens einem multiregionalen Trail konfiguriert sein	CloudTrail1.	2.1	CloudTrail2.	3.1	CloudTrail1.	3.1	CloudTrail1.
ASR-EnableEncryption CloudTrail sollte die Verschlüsselung im Ruhezustand aktiviert haben	CloudTrail2.	2.7	CloudTrail1.	3.7	CloudTrail2.	3.5	CloudTrail2.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnableLogFileValidation Stellen CloudTrail Sie sicher, dass die Überprüfung der Protokolldatei aktiviert ist	CloudTrail4.	2.2	CloudTrail3.	3.2	CloudTrail4.		CloudTrail4.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnableCloudTrailToCloudWatchLogging Stellen Sie sicher, dass CloudTrail Trails in Amazon CloudWatch Logs integriert sind	CloudTrail5.	2.4	CloudTrail4.	3.4	CloudTrail5.		CloudTrail5.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-konfiguriert 3 BucketLogging Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem S3-Bucket aktiviert ist CloudTrail		2.6		3.6		3.4	CloudTrail7.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-ReplaceCodeBuildClearTextCredentials CodeBuild Projektumgebungsvariablen sollten keine Klartext-Anmeldeinformationen enthalten	CodeBuild 2.		CodeBuild 2.		CodeBuild 2.		CodeBuild 2.
ASR-aktivierenAWSConfig Stellen Sie sicher, dass AWS Config aktiviert ist	Config.1	2.5	Config.1	3.5	Config.1	3.3	Config.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR Als privat kennzeichnen EBSSnapshots Amazon EBS-Snapshots sollten nicht öffentlich wiederherstellbar sein	EC21.		EC21.		EC21.		EC21.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EntfernenVPCDefaultSecurityGroupRules Die VPC-Standardsicherheitsgruppe sollte eingehenden und ausgehenden Datenverkehr verbieten	EC22.	4.3	EC22.	5.3	EC22.	5.4	EC22.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-fähige Protokolle VPCFlow Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs	EC26.	2,9	EC2.6	3.9	EC2.6	3.7	EC2.6
ASR-EnableEbsEncryptionByDefault Die EBS-Standardverschlüsselung sollte aktiviert sein	EC27.	2.2.1			EC2.7	2.2.1	EC2.7

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-RevokeUnrotatedKeys Die Zugangsschlüssel der Benutzer sollten alle 90 Tage oder weniger gewechselt werden	IAM.3	1.4		1.14	IAM.3	1.14	IAM.3
ASR-Set-Richtlinie IAMPasswo rd IAM-Standardkennwortrichtlinie	IAM.7	1.5-1.11	IAM.8	1.8	IAM.7	1.8	IAM.7

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-Anmeldeinformationen RevokeUnused IAMUser Benutzeranmeldedaten sollten deaktiviert werden, wenn sie nicht innerhalb von 90 Tagen verwendet werden	IAM.8	1.3	IAM.7		IAM.8		IAM.8

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-Anmeldeinformationen RevokeUnused IAMUser Benutzeranmeldedaten sollten deaktiviert werden, wenn sie nicht innerhalb von 45 Tagen verwendet werden				1.12		1.12	IAM.22

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-RemoveLambdaPublicAccess Lambda-Funktionen sollten den öffentlichen Zugriff verbieten	Lambda.1		Lambda.1		Lambda.1		Lambda.1
ASR Als privat kennzeichnen RDSSnapshot RDS-Snapshots sollten den öffentlichen Zugriff verbieten	RDS.1		RDS.1		RDS.1		RDS.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-DisablePublicAccessToRDSInstance RDS-DB-Instances sollten den öffentlichen Zugriff verbieten	RDS.2		RDS.2		RDS.2	2.3.3	RDS.2

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-verschlüsseln RDSSnapshot RDS-Cluster-Snapshots und Datenbank-Snapshots sollten im Ruhezustand verschlüsselt werden	RDS.4				RDS.4		RDS.4

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnableMulti AZOnRDSInstance RDS-DB-Instances sollten mit mehreren Availability Zones konfiguriert werden	RDS.5				RDS.5		RDS.5

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnableEnhancedMonitoringOnRDSInstance Die erweiterte Überwachung sollte für RDS-DB-Instances und -Cluster konfiguriert werden	RDS.6				RDS.6		RDS.6

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-fähig RDSCluster DeletionProtection Für RDS-Cluster sollte der Löschschutz aktiviert sein	RDS.7				RDS.7		RDS.7
ASR-aktiviert RDSInstance DeletionProtection Für RDS-DB-Instances sollte der Löschschutz aktiviert sein	RDS.8				RDS.8		RDS.8

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnableMinorVersionUpgradeOnRDSDBInstance Automatische RDS-Upgrades für kleinere Versionen sollten aktiviert sein	RDS.13				RDS.13	2.3.2	RDS.13

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnableCopyTagsToSnapshotOnRDSCluster RDS-DB-Cluster sollten so konfiguriert sein, dass sie Tags in Snapshots kopieren	RDS.16				RDS.16		RDS.16

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-DisablePublicAccessToRedshiftCluster Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten	Redshift.1		Redshift.1		Redshift.1		Redshift.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnableAutomaticSnapshotsOnRedshiftCluster Amazon Redshift Redshift-Clustern sollten automatische Snapshots aktiviert sein	Redshift.3				Redshift.3		Redshift.3

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnableRedshiftClusterAuditLogging Amazon Redshift Redshift-Cluster sollte die Audit-Protokollierung aktiviert sein	Redshift.4				Redshift.4		Redshift.4

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnableAutomaticVersionUpgradeOnRedshiftCluster Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein	Redshift.6				Redshift.6		Redshift.6

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-konfiguriert 3 PublicAccessBlock Die Einstellung S3 Block Public Access sollte aktiviert sein	S3.1	2.3	S3.6	2.1.5.1	S3.1	2.1.4	S3.1
ASR-konfiguriert 3 BucketPublicAccessBlock S3-Buckets sollten öffentlichen Lesezugriff verbieten	S3.2		S3.2	2.1.5.2	S3.2		S3.2

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-konfiguriert 3 BucketPublicAccessBlock S3-Buckets sollten öffentlichen Schreibzugriff verbieten		S3.3					S3.3
ASR- S3 EnableDefaultEncryption Bei S3-Buckets sollte die serverseitige Verschlüsselung aktiviert sein	S3.4		S3.4	2.1.1	S3.4		S3.4

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-Set-Richtlinie SSLBucket S3-Buckets sollten Anfragen zur Verwendung von SSL erfordern	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-S3 BlockDenylist Amazon S3 S3-Berechtigungen, die anderen AWS-Konten in Bucket-Richtlinien gewährt wurden, sollten eingeschränkt werden	S3.6				S3.6		S3.6
Die Einstellung S3 Block Public Access sollte auf Bucket-Ebene aktiviert sein	S3.8				S3.8		S3.8

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-konfiguriert 3 BucketPublicAccessBlock Stellen Sie sicher, dass der S3-Bucket, auf den die CloudTrail Anmeldung erfolgt, nicht öffentlich zugänglich ist		2.3					CloudTrail6.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-CreateAccessLoggingBucket Stellen Sie sicher, dass die Protokollierung des S3-Bucket-Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist		2.6					CloudTrail7.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnableKeyRotation Stellen Sie sicher, dass die Rotation für vom Kunden erstellte Dateien aktiviert CMKs ist		2.8	KMS.1	3.8	KMS.4	3.6	KMS.4

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind		3.1		4.1			Wolkenbeobachtung.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung in der AWS-Managementkonsole ohne MFA vorhanden sind		3.2		4.2			Cloudwatch.2

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für die Verwendung des Root-Benutzers vorhanden sind		3.3	CW.1	4.3			Cloudwatch.3

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der IAM-Richtlinie vorhanden sind		3.4		4.4			Cloudwatch.4

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind		3.5		4.5			Cloudwatch.5

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für Authentifizierungsfehler in der AWS Management Console vorhanden sind		3.6		4.6			Cloudwatch.6

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind, um vom Kunden erstellte Dateien zu deaktivieren oder zu löschen CMKs		3.7		4.7			Cloudwatch.7

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind		3.8		4,8			Cloudwatch.8

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für Änderungen der AWS Config vorhanden sind		3.9		4,9 bis 4,9			Cloudwatch.9

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Sicherheitsgruppe vorhanden sind		3,10		4,10			Cloudwatch.10

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind		3,11		4,11			Cloudwatch.11

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an Network-Gateways vorhanden sind		3,12		4,12			Cloudwatch.12

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Routing-Tabelle vorhanden sind		3.13		4,13			Cloudwatch.13

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-CreateLogMetricFilterAndAlarm Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für VPC-Änderungen vorhanden sind		3,14		4,14			Cloudwatch.14

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
AWS-DisablePublicAccessForSecurityGroup Stellen Sie sicher, dass keine Sicherheitsgruppen den Zugang von 0.0.0.0/0 zu Port 22 zulassen		4.1	EC25.		EC21.3		EC2.13

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
AWS-DisablePublicAccessForSecurityGroup Stellen Sie sicher, dass keine Sicherheitsgruppen den Zugang von 0.0.0.0/0 zu Port 3389 zulassen		4.2			EC2.14		EC2.14
ASR-Konfiguration SNSTopicForStack	CloudFormation1.				CloudFormation1.		CloudFormation1.
ASR-Rolle erstellen IAMSupport		1.20		1,17		1,17	IAM.18

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-ZuweisenDisablePublicIPAuto EC2 Amazon-Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen	EC21.5				EC2.15		EC2.15
ASR-EnableCloudTrailLogFileValidation	CloudTrail4.	2.2	CloudTrail3.	3.2			CloudTrail4.
ASR-EnableEncryptionFor SNSTopic	SNS.1				SNS.1		SNS.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnableDeliveryStatusLoggingForSNSTopic Die Protokollierung des Zustellungsstatus sollte für Benachrichtigungen aktiviert sein, die an ein Thema gesendet werden	SNS.2				SNS.2		SNS.2
ASR-EnableEncryptionFor SQSQueue	SQS.1				SQS.1		SQS.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-MakeRDSSnapshotPrivate RDS-Snapshot sollte privat sein	RDS.1		RDS.1				RDS.1
ASR-BlockSSMDocumentPublicAccess SSM-Dokumente sollten nicht öffentlich sein	SSM.4				SSM.4		SSM.4

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnableCloudFrontDefaultRootObject CloudFront Bei Distributionen sollte ein Standard-Root-Objekt konfiguriert sein	CloudFront1.				CloudFront1.		CloudFront1.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-SetCloudFrontOriginDomain CloudFront Verteilungen sollten nicht auf nicht existierende S3-Ursprünge verweisen	CloudFront.2				CloudFront.12		CloudFront.12

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-RemoveCodeBuildPrivilegedMode CodeBuild Projektumgebungen sollten eine protokollierende AWS-Konfiguration haben	CodeBuild 5.				CodeBuild 5.		CodeBuild 5.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-Instanz beenden EC2 Gestoppte EC2 Instanzen sollten nach einem bestimmten Zeitraum entfernt werden	EC24.				EC24.		EC24.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-aktiviert IMDSV2 OnInstance EC2 Instanzen sollten Instance Metadata Service Version 2 () verwenden IMDSv2	EC2.8				EC2.8	5.6	EC2.8

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-RevokeUnauthorizedInboudRules Sicherheitsgruppen sollten nur uneingeschränkten eingehenden Verkehr für autorisierte Ports zulassen	EC21.8				EC2.18		EC2.18

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
HIER DEN TITEL EINFÜGEN Sicherheitsgruppen sollten keinen uneingeschränkten Zugriff auf Ports mit hohem Risiko zulassen	EC21.9				EC2.19		EC2.19

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-deaktivieren TGWAutoAcceptSharedAttachments Amazon EC2 Transit Gateways sollte VPC-Anhangsanfragen nicht automatisch akzeptieren	EC22.3				EC22,3		EC22,3

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnablePrivateRepositoryScanning Bei privaten ECR-Repositorys sollte das Scannen von Bildern konfiguriert sein	ECR.1				ECR.1		ECR.1
ASR-EnableGuardDuty GuardDuty sollte aktiviert sein	GuardDuty 1.		GuardDuty 1.		GuardDuty 1.		GuardDuty 1.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-Configures3BucketLogging Die Protokollierung des S3-Bucket-Servers sollte aktiviert sein	S3.9				S3.9		S3.9
ASR-EnableBucketEventNotifications Bei S3-Buckets sollten Ereignisbenachrichtigungen aktiviert sein	S3.11				S3.11		S3.11

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-Sets3 Lifecycle Policy Für S3-Buckets sollten Lebenszyklusrichtlinien konfiguriert sein	S3.13				S3.13		S3.13
ASR-EnableAutoSecretRotation Secrets Manager Manager-Geheimnissen sollte die automatische Rotation aktiviert sein	SecretsManager1.				SecretsManager1.		SecretsManager1.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-RemoveUnusedSecret Unbenutzte Secrets Manager Manager-Geheimnisse entfernen	SecretsManager3.				SecretsManager3.		SecretsManager3.
ASR-UpdateSecretRotationPeriod Secrets Manager Manager-Geheimnisse sollten innerhalb einer bestimmten Anzahl von Tagen rotiert werden	SecretsManager4.				SecretsManager4.		SecretsManager4.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-aktiviert APIGateway CacheData Encryption API-Gateway-REST-API-Cache-Daten sollten im Ruhezustand verschlüsselt werden					APIGateway5.		APIGateway5.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-SetLogGroupRetentionDays CloudWatch Protokollgruppen sollten für einen bestimmten Zeitraum aufbewahrt werden					CloudWatch1.6		CloudWatch.16

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-AttachServiceVPCEndpoint Amazon EC2 sollte für die Verwendung von VPC-Endpunkten konfiguriert sein, die für den Amazon-Service erstellt wurden EC2	EC21.0				EC2.10		EC2.10

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-TagGuardDutyResource GuardDuty Filter sollten markiert werden							GuardDuty 2.
ASR-TagGuardDutyResource GuardDuty Detektoren sollten markiert werden							GuardDuty 4.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-Anhängen SSMPermissions an EC2 EC2 Amazon-Instances sollten von Systems Manager verwaltet werden	SSM.1		SSM.3				SSM.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-ConfigureLaunchConfigNoPublicIPDocument EC2 Amazon-Instances, die mit Auto Scaling Scaling-Gruppenstartkonfigurationen gestartet wurden, sollten keine öffentlichen IP-Adressen haben					AutoScaling.5		AutoScaling.5

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-aktivieren APIGateway Execution Logs	APIGateway1.						APIGateway1.
ASR-EnableMacie Amazon Macie sollte aktiviert sein	Macie.1				Macie.1		Macie.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnableAthenaWorkGroupLogging Athena Athena-Arbeitsgruppen sollte die Protokollierung aktiviert sein	Athena.4						Athena.4

Descripti on	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherhei tskontrol le
ASR-Enfor ce ALB HTTPSFor Der Applicati on Load Balancer sollte so konfiguri ert sein, dass alle HTTP-Anfr agen an HTTPS umgeleite t werden	ELB.1		ELB.1		ELB.1		ELB.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-Limit ECSRoot FilesystemAccess ECS-Container sollten auf den schreibgeschützten Zugriff auf Root-Dateisysteme beschränkt sein	ECS.5				ECS.5		ECS.5

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnableElastiCacheBackups ElastiCache Bei Clustern (Redis OSS) sollten automatische Backups aktiviert sein	ElastiCache1.				ElastiCache1.		ElastiCache1.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnableElastiCacheVersionUpgrades ElastiCache Bei Clustern sollten automatische Upgrades für kleinere Versionen aktiviert sein	ElastiCache2.				ElastiCache2.		ElastiCache2.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-EnableElastiCacheReplicationGroupFailover ElastiCache Für Replikationsgruppen sollte automatisches Failover aktiviert sein	ElastiCache3.				ElastiCache3.		ElastiCache3.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-Skalierung Configure DynamoDBAuto DynamoDB Tabellen sollten die Kapazität automatisch bei Bedarf skalieren	DynamoDB.1				DynamoDB.1		DynamoDB.1
ASR-Ressource TagDynamoDBTable DynamoDB Tabellen sollten mit Tags versehen werden							DynamoDB.5

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS Version 1.4.0	NIST	CIS v3.0.0	ID für die Sicherheitskontrolle
ASR-Schutz EnableDynamo DBDeletion DynamoDB DynamoDB Tabellen sollte der Löschschutz aktiviert sein					Dynamo DB,6		Dynamo DB,6

Neue Abhilfemaßnahmen hinzufügen

Abhilfemaßnahmen können manuell hinzugefügt werden, indem die entsprechenden Playbook-Dateien aktualisiert werden, oder programmgesteuert, indem die Lösung um CDK-Konstrukte erweitert wird, je nach Ihrem bevorzugten Workflow.

> **Note**
>
> In den folgenden Anweisungen werden die von der Lösung installierten Ressourcen als Ausgangspunkt verwendet. Konventionell enthalten die meisten Lösungsressourcennamen ASR and/or SO0111, um sie leicht auffinden und identifizieren zu können.

Überblick über den manuellen Arbeitsablauf

Automated Security Response auf AWS-Runbooks muss der folgenden Standardbenennung folgen:

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

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

Version: Die Version des Standards. Auch dies muss mit der von ASR unterstützten Version und der Version in den Ergebnisdaten übereinstimmen.

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

1. Erstellen Sie ein Runbook in dem/den Mitgliedskonto (en).
2. Erstellen Sie eine IAM-Rolle in dem/den Mitgliedskonto (en).
3. (Optional) Erstellen Sie eine Regel zur automatischen Problembehebung im Administratorkonto.

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

1. Melden Sie sich bei der AWS Systems Manager Manager-Konsole an und erhalten Sie ein Beispiel für das gefundene JSON.
2. Erstellen Sie ein Automatisierungs-Runbook, das den Befund behebt. Verwenden Sie auf der Registerkarte „Mein Eigentum“ eines der `ASR-` Dokumente auf der Registerkarte „Dokumente“ als Ausgangspunkt.
3. Die AWS Step Functions im Administratorkonto führen Ihr Runbook aus. Ihr Runbook muss die Behebungsrolle angeben, damit sie beim Aufrufen des Runbooks übergeben wird.

Schritt 2. Erstellen Sie eine IAM-Rolle in den Mitgliedskonten

1. Melden Sie sich bei der AWS Identity and Access Management-Konsole an.
2. Rufen Sie ein Beispiel aus den IAM SO0111-Rollen ab und erstellen Sie eine neue Rolle. Der Rollenname muss mit SO0111-Remediate- - - beginnen. *<standard>* *<version>* *<control>* Wenn Sie zum Beispiel CIS v1.2.0 Control 5.6 hinzufügen, muss die Rolle `SO0111-Remediate-CIS-1.2.0-5.6`
3. Erstellen Sie anhand des Beispiels eine Rolle mit einem angemessenen Gültigkeitsbereich, die nur die für die Problembehebung erforderlichen API-Aufrufe zulässt.

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

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

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

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

Überblick über den CDK-Workflow

Zusammenfassend werden die folgenden Dateien im ASR-Repo geändert oder hinzugefügt. In diesem Beispiel wurde den SC- und AFSBP-Playbooks eine neue Problembehebung für ElastiCache .2 hinzugefügt.

> **Note**
>
> Alle neuen Behebungen sollten dem SC-Playbook hinzugefügt werden, da es alle in ASR verfügbaren Behebungen konsolidiert. Wenn Sie beabsichtigen, nur einen bestimmten Satz von Playbooks (z. B. AFSBP) bereitzustellen, können Sie entweder: (1) die Behebung nur Ihren beabsichtigten Playbooks hinzufügen oder (2) die Behebung zusätzlich zum SC-Playbook allen Playbooks hinzufügen, für die sie im entsprechenden Security Hub Hub-Standard existiert. Die zweite Option wird aus Gründen der Flexibilität empfohlen.

In diesem Beispiel ist ElastiCache .2 in den folgenden Security Hub Hub-Standards enthalten:

- AFSBP
- NIST.800-53.R5 SI-2

- NIST.800-53,R5 SI-2 (2)
- NIST.800-53.R5 SI-2 (4)
- NIST.800-53.R5 SI-2 (5)
- PCI-DSS v4.0.1/6.3.3

Da ASR standardmäßig nur Playbooks für AFSBP und NIST.800-53 implementiert, werden wir diese neue Lösung zusätzlich zu SC zu diesen Playbooks hinzufügen.

Modifizieren Sie

- source/lib/remediation-runbook-stack.ts
- source/playbooks/AFSBP/lib/[Standardname] _remediations.ts
- source/playbooks/NIST80053/lib/control_runbooks-construct.ts
- source/playbooks/NIST80053/lib/[Standardname] _remediations.ts
- source/playbooks/SC/lib/control_runbooks-construct.ts
- source/playbooks/SC/lib/sc_Remediations.ts
- source/test/regex_registry.ts

Addition

- source/playbooks/SC/ssmdocs/SC_ .2.ts ElastiCache
- source/playbooks/SC/ssmdocs/descriptions/ElastiCache.2.md
- source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml

> **Note**
>
> Der für das Runbook gewählte Name kann eine beliebige Zeichenfolge sein, sofern er mit den übrigen vorgenommenen Änderungen übereinstimmt.

- source/playbooks/NIST80053/ssmdocs/NIST80053_ .2.ts ElastiCache
- source/playbooks/AFSBP/ssmdocs/AFSBP_ ElastiCache .2.yaml

Schritte der Entwicklung

1. Erstellen Sie das Remediation Runbook.
2. Erstellen Sie die Control Runbooks.
3. Integrieren Sie jedes Control Runbook in ein Playbook.
4. Erstellen Sie die IAM-Rolle für die Problembehebung und integrieren Sie das Wiederherstellungs-Runbook
5. Unit-Tests aktualisieren

Schritt 1: Erstellen Sie das Remediation Runbook

Dies ist das SSM-Dokument, das zur Behebung von Ressourcen verwendet wird. Es muss den `AutomationAssumeRole` Parameter enthalten, bei dem es sich um die IAM-Rolle mit den Berechtigungen zur Ausführung der Problembehebung handelt. Sehen Sie sich die vorhandene Datei `source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml` als Referenz an, wenn Sie neue Reparatur-Runbooks erstellen.

Alle neuen Runbooks sollten dem Verzeichnis hinzugefügt werden. `source/remediation_runbooks/`

Schritt 2: Erstellen Sie die Control Runbooks

Ein Kontroll-Runbook ist ein Playbook-spezifisches Runbook, das die Ergebnisdaten aus dem angegebenen Standard analysiert und das entsprechende Remediation Runbook ausführt. Da wir den SC-, AFSBP- und NIST8 0053-Playbooks die ElastiCache 2.2-Problembehebung hinzufügen, müssen wir für jedes Playbook ein neues Kontroll-Runbook erstellen. Die folgenden Dateien werden erstellt:

- source/playbooks/SC/ssmdocs/SC_ ElastiCache .2.ts
- source/playbooks/NIST80053/ssmdocs/NIST80053_ .2.ts ElastiCache
- source/playbooks/AFSBP/ssmdocs/AFSBP_ ElastiCache .2.yaml

Example

<PLAYBOOK_NAME><CONTROL.ID>Die Benennung dieser Dateien ist wichtig und muss dem Format _ .ts/yaml folgen

Einige Playbooks in ASR unterstützen IaC-Steuerungs-Runbooks TypeScript, während andere in rohem YAML geschrieben werden müssen. Beziehen Sie sich als Beispiele auf die vorhandenen

Abhilfemaßnahmen im jeweiligen Playbook. In diesem Beispiel werden wir uns mit dem SC-Playbook befassen, das IaC verwendet.

Im SC-Playbook sollte Ihr neues Kontroll-Runbook eine Klasse exportieren, die den Namen Ihres ControlRunbookDocument Behebungs-Runbooks erweitert und diesem entspricht. Schauen Sie sich das folgende Beispiel an:

```
export class EnableElastiCacheVersionUpgrades extends ControlRunbookDocument {
  constructor(scope: Construct, id: string, props: ControlRunbookProps) {
    super(scope, id, {
      ...props,
      securityControlId: 'ElastiCache.2',
      remediationName: 'EnableElastiCacheVersionUpgrades',
      scope: RemediationScope.REGIONAL,
      resourceIdRegex: <Regex>,
      resourceIdName: 'ClusterId',
      updateDescription: new StringFormat('Automatic minor version upgrades enabled for
 cluster %s.', [
        StringVariable.of(`ParseInput.ClusterId`),
      ]),
    });
  }
}
```

- `securityControlId`ist die Kontroll-ID für die Korrektur, die Sie hinzufügen, so wie sie in der Ansicht der konsolidierten Kontrollen in Security Hub definiert ist.
- `remediationName`ist der Name, den Sie für Ihr Behebungs-Runbook gewählt haben.
- `scope`ist der Umfang der Ressource, die Sie korrigieren, und gibt an, ob sie global oder in einer bestimmten Region vorhanden ist.
- `resourceIdRegex`ist der reguläre Ausdruck, der verwendet wird, um die Ressourcen-ID zu erfassen, die Sie als Parameter an das Reparatur-Runbook übergeben möchten. Es sollte nur eine Gruppe erfasst werden, alle anderen Gruppen sollten nicht erfasst werden. Wenn Sie den gesamten ARN übergeben möchten, lassen Sie dieses Feld weg.
- `resourceIdName`ist der Name, den Sie für die Ressourcen-ID festlegen möchten`resourceIdRegex`, mit der Sie erfasst wurden. Dieser Name sollte mit dem Namen des Ressourcen-ID-Parameters in Ihrem Behebungs-Runbook übereinstimmen.
- `updateDescription`ist die Zeichenfolge, die Sie dem Abschnitt „Notizen“ des Ergebnisses in Security Hub zuweisen möchten, sobald die Behebung erfolgreich ist.

Sie müssen auch eine aufgerufene Funktion exportierencreateControlRunbook, die eine neue Instanz Ihrer Klasse zurückgibt. Für ElastiCache .2 sieht das so aus:

```
export function createControlRunbook(scope: Construct, id: string, props:
 PlaybookProps): ControlRunbookDocument {
  return new EnableElastiCacheVersionUpgrades(scope, id, { ...props, controlId:
 'ElastiCache.2' });
}
```

wo `controlId` ist die Kontroll-ID, wie sie im Sicherheitsstandard definiert ist, der dem Playbook zugeordnet ist, unter dem Sie arbeiten.

Wenn das Security Hub-Steuerelement Parameter enthält, die Sie an Ihr Behebungs-Runbook übergeben möchten, können Sie sie übergeben, indem Sie Überschreibungen zu den folgenden Methoden hinzufügen: -`getExtraSteps`: definiert Standardwerte für jeden Parameter, der für das Steuerelement in Security Hub implementiert ist.

> **Note**
>
> Jedem Parameter von Security Hub muss ein Standardwert zugewiesen werden

- `getInputParamsStepOutput`: definiert die Ausgaben für den GetInputParams Schritt des Kontroll-Runbooks
- Jede Ausgabe hat ein `name`output`Type`, und`selector`. Der `selector` sollte derselbe Selektor sein, der bei der `getExtraSteps` Methodenüberschreibung verwendet wurde.
- `getRemediationParams`: definiert die Parameter, die an das Behebungs-Runbook übergeben und aus den Ausgaben der Schritte abgerufen werden. GetInputParams

Um ein Beispiel anzuzeigen, navigieren Sie zu der Datei. `source/playbooks/SC/ssmdocs/SC_DynamoDB.1.ts`

Schritt 3: Integrieren Sie jedes Control Runbook in ein Playbook

Für jedes Kontroll-Runbook, das im vorherigen Schritt erstellt wurde, müssen Sie es jetzt in die Infrastrukturdefinitionen im zugehörigen Playbook integrieren. Gehen Sie für jedes Kontroll-Runbook wie folgt vor.

> **Important**
>
> Wenn Sie das Kontroll-Runbook mit rohem YAML anstelle von Typoskript-IaC erstellt haben, fahren Sie mit dem nächsten Abschnitt fort.

Unter `/<playbook_name>/control_runbooks-construct.ts` Importieren Sie Ihre neu erstellte Kontroll-Runbook-Datei wie folgt:

```
import * as elasticache_2 from '../ssmdocs/SC_ElastiCache.2';
```

Gehen Sie als Nächstes zum Array für

```
const controlRunbooksRecord: Record<string, any>
```

Und fügen Sie einen neuen Eintrag hinzu, der die Kontroll-ID (Playbook-spezifisch) der von Ihnen erstellten `createControlRunbook` Methode zuordnet:

```
'ElastiCache.2': elasticache_2.createControlRunbook,
```

Fügen Sie die Playbook-spezifische Kontroll-ID wie folgt zur Liste der Korrekturen hinzu: `<playbook_name>\_remediations.ts`

```
{ control: 'ElastiCache.2', versionAdded: '2.3.0' },
```

Das `versionAdded` Feld sollte die neueste Version der Lösung sein. Wenn das Hinzufügen der Korrektur gegen die Größenbeschränkung der Vorlage verstößt, erhöhen Sie den. `versionAdded` Sie können die Anzahl der Behebungen, die in jedem Playbook-Mitgliedsstapel enthalten sind, anpassen. `solution_env.sh`

Schritt 4: Erstellen Sie die IAM-Rolle für die Problembehebung und integrieren Sie das Runbook

Jede Problembehebung hat ihre eigene IAM-Rolle mit benutzerdefinierten Berechtigungen, die zur Ausführung des Wiederherstellungs-Runbooks erforderlich sind. Darüber hinaus muss die `RunbookFactory.createRemediationRunbook` Methode aufgerufen werden, um das in Schritt 1 erstellte Behebungs-Runbook zu den Vorlagen der Lösung hinzuzufügen. CloudFormation

In der `remediation-runook-stack.ts` hat jede Korrektur ihren eigenen Codeblock in der Klasse. `RemediationRunbookStack` Der folgende Codeblock zeigt die Erstellung einer neuen IAM-Rolle und die Standardisierungs-Runbook-Integration für die 2.2-Behebung: ElastiCache

```
    //-----------------------
    // EnableElastiCacheVersionUpgrades
    //
    {
      const remediationName = 'EnableElastiCacheVersionUpgrades'; // should match the
 name of your remediation runbook
      const inlinePolicy = new Policy(props.roleStack, `ASR-Remediation-Policy-
${remediationName}`);

      const remediationPolicy = new PolicyStatement();
      remediationPolicy.addActions('elasticache:ModifyCacheCluster');
      remediationPolicy.effect = Effect.ALLOW;
      remediationPolicy.addResources(`arn:${this.partition}:elasticache:*:
${this.account}:cluster:*`);
      inlinePolicy.addStatements(remediationPolicy);

      new SsmRole(props.roleStack, 'RemediationRole ' + remediationName, { // creates
 the remediation IAM role
        solutionId: props.solutionId,
        ssmDocName: remediationName,
        remediationPolicy: inlinePolicy,
        remediationRoleName: `${remediationRoleNameBase}${remediationName}`,
      });

      RunbookFactory.createRemediationRunbook(this, 'ASR ' + remediationName, { // adds
 the remediation runbook to the solution's cloudformation templates
        ssmDocName: remediationName,
        ssmDocPath: ssmdocs,
        ssmDocFileName: `${remediationName}.yaml`,
        scriptPath: `${ssmdocs}/scripts`,
        solutionVersion: props.solutionVersion,
        solutionDistBucket: props.solutionDistBucket,
        solutionId: props.solutionId,
        namespace: namespace,
      });
    }
```

Schritt 5: Unit-Tests aktualisieren

Wir empfehlen, die Komponententests zu aktualisieren und auszuführen, nachdem eine neue Problembehebung hinzugefügt wurde.

Zunächst müssen Sie der `source/test/regex_registry.ts` Datei alle neuen regulären Ausdrücke (die noch nicht hinzugefügt wurden) hinzufügen. Diese Datei erzwingt Tests für jeden neuen regulären Ausdruck, der in den Runbooks der Lösung enthalten ist. Sehen Sie sich die `addElastiCacheClusterTestCases` Funktion als Beispiel an, mit der reguläre Ausdrücke getestet werden, die bei ElastiCache Problembehebungen verwendet werden.

Schließlich müssen Sie die Snapshots für jeden Stapel aktualisieren. Snapshots sind versionsgesteuerte CloudFormation Vorlagendefinitionen, die verwendet werden, um Änderungen an der ASR-Infrastruktur nachzuverfolgen. Sie können diese Snapshot-Dateien aktualisieren, indem Sie den folgenden Befehl im Verzeichnis ausführen: `deployment`

```
./run-unit-tests.sh update
```

Jetzt sind Sie bereit, Ihre neue Problembehebung einzusetzen! Im Abschnitt Build and Deploy weiter unten finden Sie Anweisungen zum Erstellen und Bereitstellen der Lösung mit Ihren neuen Änderungen.

Ein neues Playbook hinzufügen

Laden Sie die Automated Security Response on AWS-Lösungsplaybooks und den Bereitstellungsquellcode aus dem GitHub Repository herunter.

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

AWS Systems Manager Parameter Store

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

Name	Wert	Verwenden Sie
`/Solutions/SO0111/CMK_REMEDIATION_ARN`	AWS-KMS-Schlüssel, der Daten für FSBP-Problembehebungen verschlüsselt	Verschlüsselung von Kundendaten wie CloudTrail Protokollen im Rahmen von Abhilfemaßnahmen
`/Solutions/SO0111/CMK_ARN`	AWS-KMS-Schlüssel, den ASR zum Verschlüsseln von Daten verwendet	Verschlüsselung von Lösungsdaten
`/Solutions/SO0111/SNS_Topic_ARN`	ARN des Amazon SNS SNS-Themas für die Lösung	Benachrichtigung über Behebungsereignisse
`/Solutions/SO0111/SNS_Topic_Config.1`	SNS-Thema für AWS Config-Updates	Behebung von Config.1
`/Solutions/SO0111/version`	Version der Lösung	
`/Solutions/SO0111/`*`<security standard long name>`*`/`*`<version>`* /Status	`enabled`	Gibt an, ob der Standard in der Lösung aktiv ist. Ein Standard kann für automatische Problembehebungen deaktiviert werden, indem dieser Wert wie folgt geändert wird `disabled`
`/Solutions/SO0111` // Kurzname *`<security standard long name>`*	`String`	Kurzname für den Sicherheitsstandard. Zum Beispiel: `CIS`,`AFSBP`, `PCI`
`/Solutions/SO0111//`*`<security standard long name><version>`* /*`<control>`* /remap	`String`	Wenn ein Steuerelement dieselbe Korrektur wie ein anderes verwendet, führen diese Parameter die Neuzuweisung durch

Name	Wert	Verwenden Sie
`/ASR/Filters/AccountFilterMode`	Einschließen, Ausschließen oder Deaktiviert	Steuert das Verhalten der Konto-ID-Filterung für vollautomatische Problembehebungen
`/ASR/Filters/AccountFilters`	Kommagetrennte Liste von AWS-Konten IDs	Liste der AWS-Konten, IDs für die die Lösung automatische Problembehebungen filtern soll.
`/ASR/Filters/OUFilterMode`	Einschließen, Ausschließen oder Deaktiviert	Steuert das Filterverhalten der Organisationseinheiten (OUs) für vollautomatische Problembehebungen
`/ASR/Filters/OUFilters`	Durch Kommas getrennte Liste mit IDs von Organisationseinheiten	Liste der Fälle, OUs nach denen die Lösung automatische Problembehebungen filtern sollte.
`/ASR/Filters/TagFilterMode`	Einschließen, Ausschließen oder Deaktiviert	Steuert das Filterverhalten von Resource Tags für vollautomatische Problembehebungen
`/ASR/Filters/TagFilters`	Durch Kommas getrennte Liste von Resource-Tag-Schlüsseln	Liste der Ressourcen-Tag-Schlüssel, nach denen die Lösung automatisierte Problembehebungen filtern sollte.

Amazon SNS SNS-Thema — Fortschritt der Problembehebung

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

```
Remediation queued for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
Remediation failed for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
[.replaceable]`<control_ID>` remediation was successfully invoke via AWS Systems
 Manager in account [.replaceable]`<account_ID>`
```

Dies ist die Abschlussnachricht. Es weist darauf hin, dass die Wiederherstellung ohne Fehler abgeschlossen wurde. Der endgültige Test für eine erfolgreiche Wiederherstellung ist jedoch die and/or manuelle Überprüfung durch den AWS Config-Check.

Ein Abonnement für ein SNS-Thema filtern

Filterrichtlinien für Amazon SNS SNS-Abonnements:

1. Navigieren Sie zum Abonnement des SNS-Themas.
2. Wählen Sie unter Abonnementfilterrichtlinie die Option „Bearbeiten“ aus.
3. Erweitern Sie „Abonnementfilterrichtlinie“ und aktivieren Sie die Option „Abonnementfilterrichtlinie“, um Filter zu aktivieren.
4. Wählen Sie den Bereich „Nachrichtentext“ aus.
5. Fügen Sie Ihre Richtlinie dem JSON-Editor hinzu.
6. Speichern Sie die Änderungen.

Beispielrichtlinien:

Nach Konto filtern

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

Nach Fehlern filtern

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

Nach Steuerelementen filtern

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

Amazon SNS SNS-Thema — Alarme CloudWatch

Diese Lösung erstellt ein Amazon SNS SNS-Thema,`SO0111-ASR_Alarm_Topic`. Dieses Thema wird verwendet, um Alarmmeldungen zu veröffentlichen.

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

Runbook bei Konfigurationsergebnissen starten

Diese Lösung kann Runbooks auf der Grundlage von benutzerdefinierten AWS Config-Ergebnissen initiieren. Dazu müssen Sie:

1. Suchen Sie den Namen der AWS Config-Regel, die Sie korrigieren möchten. Dies kann entweder in der AWS Config oder in der Feststellung gefunden werden, die Security Hub für diese Regel generiert.
2. Navigieren Sie zu AWS Systems Manager Parameter Store und wählen Sie Parameter erstellen aus.
3. Der Name Ihrer Regel sollte `/Solutions/SO0111/` [.replaceable] lauten `Rule name from Step 1`
4. Der Wert sollte wie folgt formatiert sein:

```
{
```

```
"RunbookName":"Name of SSM runbook",

"RunbookRole": "Role that Orchestrator will assume"

}
```

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

Web-Benutzeroberfläche

Die Web-Benutzeroberfläche der Lösung ermöglicht es Benutzern, die Ergebnisse von AWS Security Hub mit einem Klick zu korrigieren, frühere Abhilfemaßnahmen anzusehen und herunterzuladen und den Zugriff auf die Lösung zu delegieren.

Die Web-Benutzeroberfläche ist für die Verwendung der Lösung nicht erforderlich. Sie können alternativ vollautomatische Problembehebungen konfigurieren, um eine manuelle Ausführung zu vermeiden, oder die AWS Security Hub CSPM-Konsole nutzen, um Behebungen mithilfe der benutzerdefinierten Aktion Remediate with ASR zu starten.

> **Note**
>
> Sie müssen den `ShouldDeployWebUI` Parameter bei der Bereitstellung des Admin-Stacks auf „yes“ setzen, um die Web-UI der Lösung verwenden zu können.

Funktionsweise

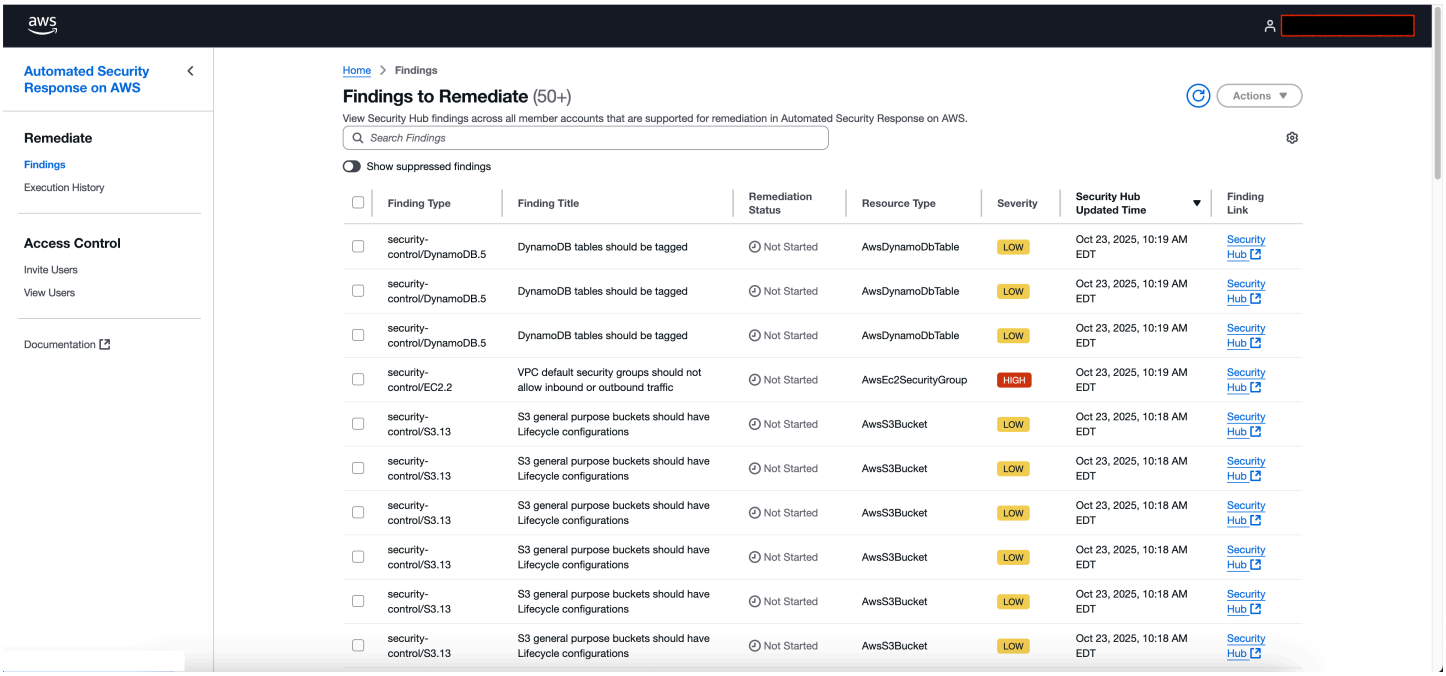
Die Web-Benutzeroberfläche der Lösung ist eine einseitige Webanwendung, die von Amazon S3 in Ihrem Konto gehostet und von Amazon vertrieben wird. CloudFront Die Lösung stellt auch eine REST-API bereit, die API Gateway verwendet, um Operationen in der Webbenutzeroberfläche zu unterstützen.

Wenn der Admin-Stack bereitgestellt wird, beginnen die Lambda-Funktionen der Lösung, alle von der Lösung unterstützten Ergebnisse von AWS Security Hub, die in Ihrem Admin-Konto vorhanden

sind, in DynamoDB zu laden. Sobald dies abgeschlossen ist, werden die auf der Weboberfläche präsentierten Ergebnisse dank der von der Lösung bereitgestellten EventBridge Regeln nahezu in Echtzeit mit Security Hub synchronisiert.

Jede Woche werden die Lambda-Funktionen der Lösung ausgelöst, um die DynamoDB-Tabelle zu aktualisieren, in der die in der Web-UI angezeigten Ergebnisse von AWS Security Hub gespeichert sind. Dadurch wird sichergestellt, dass veraltete Daten bereinigt und unsere DynamoDB-Tabellen beibehalten werden. up-to-date Wenn Sie diese Baseline so konfigurieren möchten, dass sie mehr oder weniger häufig ausgeführt wird, ändern Sie die EventBridge Regel mit dem Namen `SO0111-ASR-SynchronizationFindingsLambdaWeeklyRule` in Ihrem Administratorkonto in derselben Region, in der Sie die Lösung bereitgestellt haben.

Führen Sie Behebungen direkt in der Weboberfläche aus



Auf der Seite Ergebnisse können Admin- oder Delegated Admin-Benutzer alle Ergebnisse von AWS Security Hub einsehen, die von der Problembehebungslösung unterstützt werden. Dies schließt Ergebnisse für Security Hub Hub-Mitgliedskonten ein, die mit dem Security Hub Hub-Hauptkonto verknüpft sind. Wenn die Lösung auch in der Aggregationsregion eingesetzt wird, werden auch die Ergebnisse in jeder Onboarding-Region angezeigt. Eine Liste der von der Lösung unterstützten Ergebnisse finden Sie im Abschnitt Playbooks.

Benutzer des Kontobetreibers können nur Ergebnisse einsehen, die ihren Ursprung in AWS-Konten haben, auf die sie gemäß der Definition in ihrer Einladung Zugriff haben. Darüber hinaus können sie nur Korrekturen für Ressourcen in den Konten durchführen, mit denen sie verknüpft sind.

Um Korrekturen auszuführen, wählen Sie eine beliebige Anzahl von Elementen in der Tabelle aus und klicken Sie auf Aktionen > Korrigieren. Sie können Ergebnisse auch unterdrücken, indem Sie auf Aktionen > Unterdrücken klicken. Dadurch werden die ausgewählten Ergebnisse in der Standardansicht ausgeblendet. Sie können unterdrückte Ergebnisse jederzeit anzeigen, indem Sie auf den Schalter Unterdrückte Ergebnisse anzeigen klicken.

Sobald Sie mit der Behebung eines Befundes begonnen haben, können Sie auf der Seite Ausführungsverlauf auf die Spalte Behebungsstatus klicken, während die Korrektur entweder **`Failed`** läuft **`In Progress`** oder direkt zu dieser Korrektur weitergeleitet wird.

Filtern Sie verfügbare Ergebnisse und Abhilfemaßnahmen

Sowohl auf den Seiten Ergebnisse als auch auf der Seite Ausführungshistorie können Sie die in der Tabelle angezeigten Daten nach den Spalten filtern, die in der jeweiligen Tabelle vorhanden sind.

Auf der Seite Ergebnisse können Sie beispielsweise nach Finding Type filtern, um nach bestimmten Arten von AWS Security Hub Hub-Ergebnissen (z. B. Lambda.1 oder Athena.4) zu suchen, indem Sie auf die Suchleiste klicken und Finding Type auswählen.

> **Note**
>
> Werte, die automatisch in die Suchleiste eingegeben werden, stellen keine umfassende Liste verfügbarer Daten dar. Die vorgeschlagenen Werte für die einzelnen Suchkriterien stellen nur die Daten dar, die aktuell abgerufen und in der Benutzeroberfläche angezeigt werden.

Sie können auch mehrere Attribute in einer einzigen Suche kombinieren. Beispielsweise können Sie bei Ihrer Suche sowohl den Suchtyp als auch die Ressourcen-ID verwenden, um eine logische `AND` Abfrage durchzuführen. Darüber hinaus können Sie mehrere derselben Filterkriterien anwenden, um eine logische `OR` Suche durchzuführen, z. B. Finding Type = Lambda.1 und Finding Type = Athena.4. Dieselben Prinzipien gelten für die Seite „Ausführungsverlauf“

Authentifizierung und Autorisierung in der Webbenutzeroberfläche

Die Web-Benutzeroberfläche der Lösung ist durch eine Authentifizierung geschützt, die von Amazon Cognito bereitgestellt wird. Wenn die Lösung bereitgestellt wird, werden ein Cognito-Benutzerpool, ein Cognito App Client und eine Cognito-Benutzerpool-Domäne zusammen mit der Web-UI bereitgestellt und konfiguriert. Der E-Mail-Adresse, die als Parameter für den Admin-

Stack bereitgestellt wird, werden temporäre Anmeldeinformationen zugewiesen und sie erhält Administratorzugriff auf die Web-UI.

Es gibt drei Berechtigungstypen, die den Zugriff eines Benutzers auf die Web-UI definieren:

Art der Erlaubnis	Zugriffsebene	Anwendungsfall
Admin.	Vollständige Kontrolle über die Webbenutzeroberfläche; kann alle Ergebnisse und Behebungen einsehen, alle Behebungen und invite/view alle Benutzer ausführen.	Wird nur dem Benutzer zugewiesen, der den Admin-Stack bereitgestellt hat, wenn er bei der CloudFormation Bereitstellung seine E-Mail-Adresse angibt.
Delegierter Administrator	Erweiterte Kontrolle in der Web-UI; kann alle Ergebnisse und Abhilfemaßnahmen einsehen, alle Korrekturmaßnahmen durchführen und Benutzer des invite/view Kontobetreibers anzeigen. Administratoren und delegierte Administratoren können in der Webbenutzeroberfläche nicht eingeladen oder angezeigt werden.	Der Admin-Benutzer kann den Zugriff auf die Lösung delegieren, indem er delegierte Admin-Benutzer einlädt, die dann in der Lage sind, alle Problembehebungen durchzuführen und zu verwalten.
Kontobetreiber	Eingeschränkte Kontrolle über die Webbenutzeroberfläche; beschränkt auf die Anzeige und Korrektur von Ergebnissen nur in Konten, mit denen sie auf Einladung verknüpft sind. Es können keine weiteren Benutzer eingeladen oder angezeigt werden.	Day-to-day Benutzer, die nur eingeschränkten Zugriff haben sollten, um Problembehebungen in einer Teilmenge der integrierten Konten durchzuführen. Administratoren oder delegierte Administratoren sind dafür verantwortlich, diese Benutzer einzuladen und

Art der Erlaubnis	Zugriffsebene	Anwendungsfall
		ihren Zuständigkeitsbereich zu definieren.

Alle Benutzer müssen von einem Administrator oder delegierten Administrator eingeladen werden, bevor sie sich bei der Weboberfläche anmelden können. Um weitere Benutzer einzuladen, kann ein Administrator oder delegierter Administrator seine E-Mail-Adresse und die Berechtigungsstufe auf der Seite „Benutzer einladen“ der Weboberfläche eingeben.

Administratoren und delegierte Administratoren können auch bestehende Benutzer anzeigen, verwalten und löschen. Um eine Liste aller Benutzer zu sehen, navigieren Sie zur Seite „Benutzer anzeigen“.

Um einen vorhandenen Benutzer zu verwalten, wählen Sie den Benutzer aus der Tabelle aus und klicken Sie auf Benutzer verwalten. Anschließend können Sie den Benutzer löschen, indem Sie auf Benutzer löschen klicken. Wenn der Benutzer ein Kontobetreiber ist, können Sie die Liste der AWS-Konten IDs , auf die er Zugriff hat, im Kontext der Lösung ändern. Das Ändern des Berechtigungstyps für einen vorhandenen Benutzer wird derzeit nicht unterstützt.

Bitte beachten Sie, dass delegierte Administratoren nur Benutzer des Kontobetreibers anzeigen und verwalten können.

Integration mit externen IdPs

Sie können den von der Lösung bereitgestellten Authentifizierungsmechanismus so anpassen, dass sich Benutzer mit Ihrem eigenen OIDC- oder SAML-Identitätsanbieter wie Okta oder Microsoft Entra ID anmelden können. Die folgenden Schritte für die Integration mit External IdPs erfordern Zugriff auf das AWS-Konto, auf dem der Admin-Stack bereitgestellt wird.

> **Important**
>
> Benutzer müssen dennoch eingeladen werden, bevor sie sich mit einem externen IdP anmelden, den Sie für die Verwendung mit der Lösung konfiguriert haben. Darüber hinaus muss die mit ihrem IdP-Profil verknüpfte E-Mail-Adresse mit der in der Einladung angegebenen E-Mail-Adresse übereinstimmen.

Schritt 1 — Suchen Sie den Benutzerpool der Lösung

Suchen Sie in der Amazon Cognito Cognito-Konsole den Benutzerpool der Lösung mit dem Namen SO0111-ASR -. UserPool

Klicken Sie auf den Namen des Benutzerpools SO0111-ASR -, um zur Übersichtsseite zu gelangen. UserPool Wählen Sie dort in der Navigationsleiste Soziale Dienste und externe Anbieter aus.

Schritt 2 — Fügen Sie Ihren Identitätsanbieter hinzu

Klicken Sie auf der Seite Soziale Netzwerke und externe Anbieter oben rechts auf die Schaltfläche Identitätsanbieter hinzufügen.

Wählen Sie je nach Ihrem Identitätsanbieter entweder OIDC oder SAML aus.

Sobald Sie Ihren Anbietertyp ausgewählt haben, werden Sie aufgefordert, Informationen zu Ihrem Identitätsanbieter einzugeben.

Füllen Sie die folgenden Felder für SAML-Anbieter aus:

1. Anbietername: Ein benutzerfreundlicher Name für Ihren Anbieter
2. IDP-initiierte SAML-Anmeldung: Wählen `Require SP-initiated SAML assertions - Recommended`
3. Quelle des Metadaten-Dokuments: Wählen Sie `Upload metadata document`
4. Metadaten-Dokument: Laden Sie Ihr von Ihrem IdP bereitgestelltes SAML-Metadatendokument hoch.
5. Klicken Sie unter Attribute zwischen Ihrem SAML-Anbieter und Ihrem Benutzerpool zuordnen auf Weiteres Attribut hinzufügen. Wählen Sie für Benutzerpool-Attribut eine Option `email` aus der Dropdownliste aus. Geben Sie unter SAML-Attribut den vollständigen Namen des Attributs ein, in dem die E-Mail-Adresse des Benutzers in Ihrem SAML-Identitätsanbieter gespeichert ist. Beispiel, `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress` .
6. Klicken Sie auf Identitätsanbieter hinzufügen, um Ihre Änderungen zu speichern.

Füllen Sie die folgenden Felder für OIDC-Anbieter aus:

1. Anbietername: Ein freundlicher Name für Ihren Anbieter

2. Client-ID: Geben Sie die Client-ID ein, die Sie von Ihrem OpenID Connect-Identitätsanbieter erhalten haben.
3. Kundengeheimnis: Geben Sie das vom OpenID Connect-Identitätsanbieter bereitgestellte Client-Geheimnis ein.
4. Autorisierte Bereiche: Geben Sie ein `openid profile email`
5. Methode zur Anforderung von Attributen: Wählen Sie `GET` oder `POST` basiert auf der Konfiguration Ihres Identity Providers.
6. Einrichtungsmethode: Wählen Sie die Aussteller-URL Ihres OIDC-Anbieters aus `Auto fill through issuer URL` und geben Sie sie ein. Sie können die Werte auch manuell eingeben.
7. Klicken Sie unter Attribute zwischen Ihrem OpenID Connect-Anbieter und Ihrem Benutzerpool zuordnen auf Weiteres Attribut hinzufügen. Wählen Sie für Benutzerpool-Attribut eine Option `email` aus der Dropdownliste aus. Geben Sie für das OpenID Connect-Attribut den vollständigen Namen des Attributs ein, in dem die E-Mail-Adresse des Benutzers in Ihrem OIDC-Identitätsanbieter gespeichert ist. Beispiel, `email`.
8. Klicken Sie auf Identitätsanbieter hinzufügen, um Ihre Änderungen zu speichern.

> **Important**
>
> Sie müssen eine Attributzuordnung für das `email` Benutzerpool-Attribut hinzufügen, auch wenn der Attributname Ihres Identitätsanbieters ebenfalls lautete`email`.

Schritt 3 — Fügen Sie Ihren Anbieter zum App Client der Lösung hinzu

Navigieren Sie zur Seite App Clients und wählen Sie den Client mit dem Namen SO0111-ASR-WebUI - aus. UserPoolClient

Klicken Sie auf den Tab Anmeldeseiten und dann unter Konfiguration der verwalteten Anmeldeseiten auf Bearbeiten.

Fügen Sie im Feld Identitätsanbieter den Identitätsanbieter hinzu, den Sie im vorherigen Schritt erstellt haben. Klicken Sie auf Save Changes (Änderungen speichern).

Schritt 4 — Konfigurieren Sie Ihren Identitätsanbieter

Damit Ihr Identitätsanbieter nach der Anmeldung zur Weboberfläche der Lösung weiterleiten kann, müssen Sie URLs in Ihrer IdP-Konfiguration Folgendes zulassen.

Abhängig von Ihrem Anbietertyp sollten Sie einen der folgenden Callbacks auf die Zulassungsliste setzen: URLs

1. SAML-Rückruf-URL: https://so0111-asr — .auth. *<your-aws-account-id>* *<aws-region>*.amazoncognito. com/saml2/idpresponse
2. URL für den OIDC-Rückruf: https://so0111-asr - .auth. *<your-aws-account-id>* *<aws-region>*.amazoncognito. com/oauth2/idpresponse

Sie sollten es durch die AWS-Konto-ID `<your-aws-account-id>` ersetzen, in der Sie den Admin-Stack bereitgestellt haben, und `<aws-region>` durch die Region, in der Sie den Admin-Stack bereitgestellt haben.

Schritt 4 — Überprüfen Sie Ihre Integration

Navigieren Sie zur Anmeldeseite der Web-Benutzeroberfläche. Vergewissern Sie sich, dass Ihr benutzerdefinierter Identitätsanbieter auf der Anmeldeseite sichtbar ist.

Um die Integration zu testen, laden Sie über die Seite „Benutzer einladen“ einen neuen Benutzer ein. Stellen Sie anschließend sicher, dass sich der Benutzer authentifizieren kann, indem Sie auf der Anmeldeseite der Web-UI auf Ihren benutzerdefinierten Identitätsanbieter klicken.

Bitte beachten Sie, dass das Benutzerprofil in Ihrem benutzerdefinierten IdP mit derselben E-Mail-Adresse verknüpft sein muss, die in der Einladung angegeben wurde. Mit anderen Worten, die E-Mail-Adresse in den Angaben Ihres Anbieters muss mit der Einladung übereinstimmen.

Referenz

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

Datenerfassung

Diese Lösung sendet Betriebsmetriken (die „Daten“) über die Verwendung dieser Lösung an AWS. Wir verwenden diese Daten, um besser zu verstehen, wie Kunden diese Lösung und die damit verbundenen Dienstleistungen und Produkte nutzen. Die Erfassung dieser Daten durch AWS unterliegt der AWS-Datenschutzerklärung.

Zugehörige Ressourcen

- Automatisierte Reaktion und Problembehebung mit AWS Security Hub
- Benchmarks der Amazon Web Services Foundation in der CIS, Version 1.2.0
- Standard für bewährte Methoden der AWS-Grundsicherheit
- Payment Card Industry Data Security Standard (PCI DSS)
- Nationales Institut für Standards und Technologie (NIST) SP 800-53 Rev. 5

Mitwirkende

Die folgenden Personen haben zu diesem Dokument beigetragen:

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

- Ryan Garay
- Thiemo Belmega
- Mykhailo Markhain
- Manish Jangid
- Andrew Stephen
- Peter DeVries
- Mukta Dadariya

Revisionen

Veröffentlichungsdatum: August 2020 (letzte Aktualisierung: Januar 2025)

Besuchen Sie CHANGELOG.md in unserem GitHub Repository, um versionsspezifische Verbesserungen und Korrekturen nachzuverfolgen.

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 Produktangebote und Praktiken von AWS 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 -Services werden „wie sie sind“ ohne ausdrückliche oder stillschweigende Garantien, Zusicherungen oder Bedingungen jeglicher Art bereitgestellt. Die Verantwortlichkeiten und Verbindlichkeiten von AWS gegenüber seinen Kunden werden durch AWS-Verträge geregelt, und dieses Dokument ist weder Teil einer Vereinbarung zwischen AWS und seinen Kunden noch ändert es diese.

Automated Security Response auf AWS ist unter den Bedingungen der Apache License Version 2.0 lizenziert, die bei The Apache Software Foundation erhältlich ist.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.