



AWS Benutzerleitfaden zur Reaktion auf Sicherheitsvorfälle



Version December 1, 2024

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

AWS Benutzerleitfaden zur Reaktion auf Sicherheitsvorfälle:

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

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

Table of Contents

Was ist Reaktion auf AWS Sicherheitsvorfälle?	1
Unterstützte Konfigurationen	1
Zusammenfassung der Funktionen	2
Überwachung und Untersuchung	2
Rationalisieren Sie die Reaktion auf Vorfälle	3
Self-Service-Sicherheitslösungen	3
Dashboard für Sichtbarkeit	3
Sicherheitslage	3
Beschleunigte Hilfe	3
Bereitschaft und Bereitschaft	3
Konzepte und Terminologie	4
Erste Schritte	7
Wählen Sie ein Mitgliedskonto aus	7
Einzelheiten zur Mitgliedschaft einrichten	8
Konten verknüpfen mit AWS Organizations	9
Richten Sie proaktive Reaktions- und Alert-Triaging-Workflows ein	9
Benutzeraufgaben	11
Dashboard	11
Verwaltung meines Incident-Response-Teams	11
Kontozuweisung zu AWS Organizations	12
Überwachung und Untersuchung	2
Vorbereitung	13
Erkennen und Analysieren	14
Enthalten	17
Ausrotten	19
Wiederherstellung	20
Bericht nach dem Vorfall	20
Fälle	22
Erstellen Sie einen AWS unterstützten Fall	22
Erstellen Sie einen selbst verwalteten Fall	24
Auf einen AWS generierten Fall antworten	25
Fälle verwalten	25
Den Fallstatus ändern	26
Den Resolver ändern	27
Aktionselemente	27

Bearbeiten eines Falls	27
Kommunikation	28
Berechtigungen	28
Anlagen	29
Tags	30
Fallaktivitäten	30
Einen Fall schließen	30
Mit Stacksets arbeiten AWS CloudFormation	31
Mitgliedschaft kündigen	37
Ressourcen zur Reaktion auf AWS Sicherheitsvorfälle kennzeichnen	39
Verwenden AWS CloudShell	40
Erlangung von Berechtigungen für IAM AWS CloudShell	40
Interaktion mit Security Incident Response mithilfe von AWS CloudShell	41
CloudTrail protokolliert	42
Informationen zur Reaktion auf Sicherheitsvorfälle finden Sie unter CloudTrail	42
Die Einträge der Security Incident Response-Protokolldatei verstehen	44
Verwalten von Konten mit AWS Organizations	47
Überlegungen und Empfehlungen	47
Vertrauenswürdiger Zugriff	48
Für die Benennung eines delegierten Security Incident Response-Administratorkontos sind Berechtigungen erforderlich	50
Benennung eines delegierten Administrators für die Reaktion auf Sicherheitsvorfälle AWS	51
Mitglieder zu AWS Security Incident Response hinzufügen	53
Mitglieder aus AWS Security Incident Response entfernen	54
Fehlerbehebung	55
Problembereiche	55
Fehler	55
Support	57
Sicherheit	58
Datenschutz bei der Reaktion auf AWS Sicherheitsvorfälle	58
Datenverschlüsselung	59
Datenschutz für den Datenverkehr zwischen Netzwerken	60
Datenverkehr zwischen Service und On-Premises-Clients und -Anwendungen	60
Datenverkehr zwischen AWS -Ressourcen in derselben Region	60
Identitäts- und Zugriffsverwaltung	61
Authentifizierung mit Identitäten	62
So funktioniert die Reaktion auf AWS Sicherheitsvorfälle mit IAM	65

Fehlerbehebung bei Identität und Zugriff auf AWS Security Incident Response	74
Verwenden von Servicerollen	76
Verwenden von serviceverknüpften Rollen	76
AWSServiceRoleForSecurityIncidentResponse	77
AWSServiceRoleForSecurityIncidentResponse_Triage	78
Unterstützte Regionen für SLRs	79
AWS Verwaltete Richtlinien	80
verwaltete Richtlinie: AWSSecurityIncidentResponseServiceRolePolicy	81
verwaltete Richtlinie: AWSSecurityIncidentResponseAdmin	82
verwaltete Richtlinie: AWSSecurityIncidentResponseReadOnlyAccess	82
verwaltete Richtlinie: AWSSecurityIncidentResponseCaseFullAccess	83
verwaltete Richtlinie: AWSSecurityIncidentResponseTriageServiceRolePolicy	84
Aktualisierungen SLRs und verwaltete Richtlinien	85
Vorfallreaktion	87
Compliance-Validierung	87
Protokollierung und Überwachung in AWS Security Incident Response	88
Ausfallsicherheit	89
Sicherheit der Infrastruktur	89
Konfigurations- und Schwachstellenanalyse	90
Serviceübergreifende Confused-Deputy-Prävention	90
Service Quotas	92
AWS Reaktion auf Sicherheitsvorfälle	92
AWS Technischer Leitfaden zur Reaktion auf Sicherheitsvorfälle	94
Überblick	94
Sind Sie Well-Architected?	94
Einführung	95
Bevor Sie beginnen	96
AWS Überblick über die Reaktion auf Vorfälle	96
Vorbereitung	103
Personen	104
Prozess	108
Technologie	116
Zusammenfassung der Vorbereitungsgegenstände	124
Operationen	130
Erkennung	131
Analyse	135
Eindämmung	140

Beseitigung	146
Wiederherstellung	148
Schlussfolgerung	150
Aktivität nach Vorfällen	151
Schaffen Sie einen Rahmen, um aus Vorfällen zu lernen	151
Legen Sie Erfolgskennzahlen fest	153
Verwenden Sie Kompromissindikatoren	157
Kontinuierliche Aus- und Weiterbildung	158
Schlussfolgerung	159
Mitwirkende	159
Anhang A: Definitionen der Cloud-Funktionen	160
Protokollierung und Ereignisse	160
Sichtbarkeit und Alarmierung	162
Automatisierung	165
Sicherer Speicher	166
Künftige und maßgeschneiderte Sicherheitsfunktionen	166
Anhang B: Ressourcen zur Reaktion auf AWS Zwischenfälle	167
Ressourcen für Playbooks	167
Forensische Ressourcen	167
Hinweise	168
Dokumentverlauf	169
.....	clxxiv

Was ist AWS Security Incident Response?

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

AWS Security Incident Response analysiert die Ergebnisse, eskaliert Sicherheitsereignisse und verwaltet Fälle, die Ihre sofortige Aufmerksamkeit erfordern. Darüber hinaus haben Sie Zugriff auf das AWS Customer Incident Response Team (CIRT), das die betroffenen Ressourcen untersucht.

Note

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

AWS Security Incident Response arbeitet mit anderen [AWS Detection and Response Services](#) zusammen und führt Sie durch den gesamten Incident-Lebenszyklus — von der Erkennung bis zur Wiederherstellung.

Inhalt

- [Unterstützte Konfigurationen](#)
- [Zusammenfassung der Funktionen](#)

Unterstützte Konfigurationen

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

- Sprache: AWS Security Incident Response ist in englischer Sprache verfügbar.
- Unterstützte AWS Regionen:

AWS Security Incident Response ist in einer Teilmenge von AWS-Regionen verfügbar. In diesen unterstützten Regionen erstellen Sie eine Mitgliedschaft, erstellen und sehen sich Fälle an und greifen auf das Dashboard zu.

- USA Ost (Ohio)
- USA West (Oregon)

- USA Ost (Virginia)
- EU (Frankfurt)
- EU (Irland)
- EU (London)
- EU (Stockholm)
- Asien-Pazifik (Singapur)
- Asia Pacific (Seoul)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Canada (Central)

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

Note

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

Zusammenfassung der Funktionen

Überwachung und Untersuchung

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

Optimieren Sie die Reaktion auf Vorfälle

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

Self-Service-Sicherheitslösungen

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

Dashboard für mehr Transparenz

Überwachen und messen Sie die Bereitschaft zur Reaktion auf Vorfälle.

Sicherheitslage

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

Beschleunigte Unterstützung

Connect AWS das Customer Incident Response Team (CIRT), um Sicherheitsvorfälle zu untersuchen, einzudämmen und Hinweise zu erhalten, wie Sie sich nach Sicherheitsvorfällen erholen können.

Bereitschaft und Einsatzbereitschaft

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

Konzepte und Terminologie

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

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

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

AWS Serviceportal zur Reaktion auf Sicherheitsvorfälle: Ein Self-Service-Portal, über das Sie Fälle von Sicherheitsereignissen einleiten und verwalten können. Die kontinuierliche Kommunikation und Berichterstattung wird durch das Ticketsystem, automatisierte Benachrichtigungen und die direkte Zusammenarbeit mit dem Serviceteam erleichtert.

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

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

Kontinuierliche Verbesserung: Die Reaktion auf AWS Sicherheitsvorfälle berücksichtigt Feedback und Erfahrungen aus früheren Projekten, um die Erkennungsmöglichkeiten, Ermittlungsprozesse und Abhilfemaßnahmen zu verbessern. AWS Security Incident Response orientiert sich auch an up-to-date den neuesten Sicherheitsbedrohungen und bewährten Verfahren, um den sich entwickelnden Sicherheitsherausforderungen zu begegnen.

Cybersicherheitsereignis: Jedes beobachtbare Ereignis in einem System oder Netzwerk, das gegen Sicherheitsrichtlinien, Richtlinien zur akzeptablen Nutzung oder Standardsicherheitspraktiken verstößt oder zu verstoßen droht.

Incident Response Team: Eine Gruppe von Personen, die bei aktiven Sicherheitsereignissen Unterstützung leisten. Für AWS unterstützte Fälle ist dies das AWS Customer Incident Response Team (CIRT).

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

Investigative Tools: Tools zur Reaktion auf AWS Sicherheitsvorfälle und dienstbezogene Rollen, mit denen der Betriebsstatus Ihres Kontos und Ihrer Ressourcen überprüft wird.

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

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

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

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

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

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

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

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

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

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

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

Erste Schritte

Inhalt

- [Wählen Sie ein Mitgliedskonto](#)
- [Einzelheiten zur Mitgliedschaft einrichten](#)
- [Ordnen Sie Konten zu AWS Organizations](#)
- [Richten Sie proaktive Reaktions- und Alert-Triaging-Workflows ein](#)

Wählen Sie ein Mitgliedskonto

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

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

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

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

Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zur Verwaltung von AWS Security Incident Response verfügen.

Spezifische Schritte zum [Hinzufügen von Berechtigungen finden Sie unter Hinzufügen und Entfernen von IAM Identitätsberechtigungen](#).

Weitere Informationen finden Sie unter [Verwaltete Richtlinien für AWS Security Incident Response](#).

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


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

Note

Die spezifischen Schritte können je nach AWS Dienst und den Aktionen, die Sie ausführen möchten, variieren.

Einzelheiten zur Mitgliedschaft einrichten

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

 **Warning**

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

- Sie können optional einen Namen für diese Mitgliedschaft auswählen.
- Im Rahmen des Workflows zur Erstellung einer Mitgliedschaft müssen Sie einen primären und einen sekundären Kontakt angeben. Diese Kontakte werden automatisch in Ihr Incident-Response-Team aufgenommen. Für eine einzelne Mitgliedschaft müssen mindestens zwei Kontakte vorhanden sein, wodurch auch sichergestellt wird, dass mindestens zwei Kontakte zum Incident-Response-Team gehören.
- Definieren Sie optionale Tags für Ihre Mitgliedschaft. Mithilfe von Tags können Sie die AWS Kosten verfolgen und nach Ressourcen suchen.

Ordnen Sie Konten zu AWS Organizations

Ihre Mitgliedschaft berechtigt zum Versicherungsschutz für alle verlinkten Geräte AWS-Konten . AWS Organizations Zugeordnete Konten werden automatisch aktualisiert, wenn Konten zu Ihrer Organisation hinzugefügt oder daraus entfernt werden.

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

Der Workflow für proaktive Reaktionen und Alert-Triaging ist eine optionale Funktion, die Sie in Ihrem Unternehmen für die Überwachung aktivierter Sicherheitsdienste aktivieren können. Wählen Sie den Schalter neben der Funktion aus, die Sie aktivieren möchten.

Wenn Sie Probleme beim Onboarding haben, [erstellen Sie bitte einen AWS Support Fall](#), um zusätzliche Unterstützung zu erhalten. Stellen Sie sicher, dass Sie Details wie die AWS-Konto ID und alle Fehler angeben, die Ihnen während des Einrichtungsvorgangs möglicherweise aufgefallen sind.

Proaktive Reaktion und Alert-Triaging: AWS Security Incident Response überwacht und untersucht Warnmeldungen, die durch Amazon- GuardDuty und Security Hub Hub-Integrationen generiert wurden. Um diese Funktion nutzen zu können, [GuardDuty muss Amazon aktiviert sein](#). AWS Security Incident Response sortiert Warnmeldungen mit niedriger Priorität mithilfe von Serviceautomatisierung, sodass sich Ihr Team auf die kritischsten Probleme konzentrieren kann. Weitere Informationen darüber, wie AWS Security Incident Response mit Amazon GuardDuty und funktioniert AWS Security Hub, finden Sie im Abschnitt [Detect and Analyze](#) des Benutzerhandbuchs.

Mit dieser Funktion kann AWS Security Incident Response die Ergebnisse aller Konten und aktiven Unterstützungen AWS-Regionen in Ihrer Organisation überwachen und untersuchen. Um diese Funktionalität zu ermöglichen, erstellt AWS Security Incident Response automatisch eine dienstbezogene Rolle für alle Mitgliedskonten innerhalb Ihres AWS Organizations Kontos. Für das Verwaltungskonto müssen Sie die dienstbezogene Rolle jedoch manuell erstellen, um die Überwachung zu aktivieren.

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

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

Benutzeraufgaben

Inhalt

- [Dashboard](#)
- [Ich verwalte mein Incident Response Team](#)
- [Kontozuweisung zu AWS Organizations](#)
- [Überwachung und Untersuchung](#)
- [Fälle](#)
- [Fälle verwalten](#)
- [Mit AWS CloudFormation Stacksets arbeiten](#)
- [Mitgliedschaft kündigen](#)

Dashboard

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

Wählen Sie `view incident response team` diese Option, um auf die Details Ihrer Teammitglieder für die Reaktion auf Vorfälle zuzugreifen.

Wählen Sie `proactive response` diese Option, um festzustellen, ob die Alert-Triaging-Funktion aktiviert ist. Wenn Sie den `alert triaging Workflow` nicht aktiviert haben, können Sie seinen Status überwachen und `Proactive Response` ihn aktivieren.


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

Ich verwalte mein Incident Response Team

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

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

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

 Note

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

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

Das Incident-Response-Team erhält eine E-Mail-Benachrichtigung zu den folgenden Ereignissen:

- Fall (erstellen, löschen, aktualisieren)
- Kommentar (erstellen, löschen, aktualisieren)
- Anlage (erstellen, löschen, aktualisieren)
- Mitgliedschaft (erstellen, aktualisieren, kündigen, fortsetzen)

Kontozuweisung zu AWS Organizations

Wenn Sie AWS Security Incident Response aktivieren, wird die Mitgliedschaft erstellt und an Ihre Bedürfnisse angepasst AWS Organizations. Alle Konten in Ihren Organizations sind auf Ihre Mitgliedschaft bei AWS Security Incident Response abgestimmt.

Weitere Informationen finden Sie unter [Konten für die Reaktion auf AWS Sicherheitsvorfälle verwalten mit AWS Organizations](#).

Überwachung und Untersuchung

AWS Security Incident Response überprüft und sortiert Sicherheitswarnungen von Amazon GuardDuty und konfiguriert dann Unterdrückungsregeln auf der Grundlage Ihrer Umgebung AWS Security Hub, um unnötige Warnungen zu verhindern. Das AWS CIRT Team untersucht die Ergebnisse, die nicht geprüft wurden, und leitet Ihr Team schnell an und leitet es an, um potenzielle Probleme schnell einzudämmen. Falls gewünscht, können Sie AWS Security Incident Response die Erlaubnis erteilen, Eindämmungsmaßnahmen in Ihrem Namen durchzuführen.

AWS Security Incident Response entspricht dem NIST 800-61r2 [Computer Security Event Handling Guide für die Reaktion auf Sicherheitsereignisse](#). Durch die Ausrichtung auf diesen Industriestandard bietet AWS Security Incident Response einen konsistenten Ansatz für das Management von Sicherheitsereignissen und hält sich an bewährte Verfahren für den Schutz und die Reaktion auf Sicherheitsvorfälle in Ihrer Umgebung. AWS

Wenn der AWS Security Incident Response Service eine Sicherheitswarnung feststellt oder Sie Sicherheitsunterstützung anfordern, AWS CIRT untersucht er das Problem. Das Team sammelt Protokollereignisse und Servicedaten wie GuardDuty Warnmeldungen, sortiert und analysiert diese Daten, führt Maßnahmen zur Behebung und Eindämmung durch und erstellt Berichte nach dem Vorfall.

Inhalt

- [Vorbereitung](#)
- [Erkennen und Analysieren](#)
- [Enthalten](#)
- [Ausrotten](#)
- [Wiederherstellung](#)
- [Bericht nach dem Vorfall](#)

Vorbereitung

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

Erkennen und Analysieren

AWS Security Incident Response überwacht, bewertet und untersucht Sicherheitsergebnisse von Amazon GuardDuty und Integrationen bis hin zu AWS Security Hub. Zu den zusätzlichen Maßnahmen, die den Umfang und die Effektivität der Überwachungs- und Ermittlungskapazitäten von AWS Security Incident Response erheblich verbessern können, gehören:

Aktivierung unterstützter Erkennungsquellen

Note

AWS Die Kosten für den Service Security Incident Response beinhalten keine Nutzungs- und sonstigen Kosten und Gebühren im Zusammenhang mit unterstützten Erkennungsquellen oder der Nutzung anderer AWS Dienste. Einzelheiten zu den Kosten finden Sie auf den Seiten der einzelnen Funktionen oder Dienste.

Amazon GuardDuty

GuardDuty ist ein Dienst zur Bedrohungserkennung, der kontinuierlich Datenquellen und Protokolle in Ihrer AWS Umgebung überwacht, analysiert und verarbeitet. Eine Aktivierung GuardDuty ist nicht erforderlich, um AWS Security Incident Response zu verwenden. Um die proaktive Reaktion und die Alert-Triaging-Funktion nutzen zu können, GuardDuty muss Amazon jedoch aktiviert sein.

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

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

Durch die Aktivierung GuardDuty erhält AWS Security Incident Response Zugriff auf wichtige Daten zur Erkennung von Bedrohungen und verbessert so die Fähigkeit, potenzielle Sicherheitsprobleme in Ihrer AWS Umgebung zu erkennen und darauf zu reagieren.

AWS Security Hub

Security Hub kann Sicherheitsergebnisse von verschiedenen AWS Diensten und unterstützten Sicherheitslösungen von Drittanbietern aufnehmen. Diese Integrationen können AWS Security

Incident Response dabei helfen, Ergebnisse anderer Erkennungstools zu überwachen und zu untersuchen.

Informationen zur Aktivierung der Integration von Security Hub mit Organizations finden Sie im [AWS Security Hub Benutzerhandbuch](#).

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

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

- [CrowdStrike — CrowdStrike Falcon](#)
- [Schnürarbeiten — Schnürarbeiten](#)
- [Trend Micro — Cloud Eins](#)

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

Analyse der Ergebnisse.

AWS Das Automatisierungs- und AWS CIRT Serviceteam für die Reaktion auf Sicherheitsvorfälle analysiert alle Ergebnisse der unterstützten Tools. Wir werden beginnen, mehr über Ihre Umgebung zu erfahren, indem wir mithilfe von AWS Support Cases mit Ihnen kommunizieren. Zum Beispiel, wenn wir herausfinden müssen, ob es sich bei einem Befund um ein erwartetes Verhalten handelt oder ob es sich um einen Vorfall handeln sollte. Wenn wir mehr über Ihre Umgebung erfahren, werden wir den Service individuell anpassen und die Anzahl der Kommunikationsvorgänge reduzieren.

Ein Ereignis melden.

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

Kommunizieren.

AWS Security Incident Response hält Sie während der Untersuchung auf dem Laufenden, indem es Ihre Sicherheitskontakte über das Veranstaltungsticket kontaktiert. Möglicherweise unterstützen mehrere Teammitglieder Ihre Veranstaltung, die alle das Veranstaltungsticket für vom Kunden bereitgestellte Inhalte und Updates verwenden. AWS

Die Kommunikation kann automatische Benachrichtigungen umfassen, wenn eine Sicherheitswarnung generiert wird, Kommunikation während der Ereignisanalyse, Einrichtung von Call Bridges, die fortlaufende Analyse von Artefakten wie Protokolldateien und die Übermittlung von Ermittlungsergebnissen an Sie während des Sicherheitsereignisses.

AWS Security Incident Response verwendet zwei verschiedene Falltypen, um mit Ihnen zu kommunizieren: Support für ausgehende Mitteilungen, um Sie über ein Ereignis zu informieren, und für Fälle zur Reaktion auf AWS Sicherheitsvorfälle, um über einen Fall zu kommunizieren, den Sie uns gemeldet haben.

AWS Supportfälle: Der Service verwendet AWS Supportfälle, um mit Ihren Teams zu kommunizieren. Wir werden für jeden Fall, AWS-Konto in dem das Ergebnis generiert wurde, Supportanfragen erstellen. Dieser Ansatz erleichtert die Kommunikation mit den verschiedenen Teams, die für die spezifischen Workloads verantwortlich sind, da sie mehr über die Ereignisse in ihren Zuständigkeitsbereichen wissen.

AWS Fälle zur Reaktion auf Sicherheitsvorfälle: Wenn wir feststellen, dass ein Ergebnis zu einem Sicherheitsvorfall eskaliert werden muss, erstellen wir einen Fall zur Reaktion auf AWS Sicherheitsvorfälle. Dadurch wird sichergestellt, dass kritische Sicherheitsprobleme angemessen behandelt und entsprechend reagiert werden.

Indem Sie sich aktiv mit diesen Mitteilungen auseinandersetzen und zeitnah reagieren, können Sie dem AWS Security Incident Response Service dabei helfen:

- Verstehen Sie Ihre Umgebung und das erwartete Verhalten besser.
- Reduzieren Sie im Laufe der Zeit Fehlalarme.
- Verbessern Sie die Genauigkeit und Relevanz von Warnmeldungen.
- Sorgen Sie für eine schnelle Reaktion auf echte Sicherheitsvorfälle.
- Denken Sie daran, dass sich die Effektivität des AWS Security Incident Response Service mit Ihrer Zusammenarbeit verbessert, was zu einer sichereren und effizienteren AWS Überwachungsumgebung führt.

Enthalten

AWS Security Incident Response arbeitet mit Ihnen zusammen, um Ereignisse einzudämmen. Sie können eine Servicerolle für AWS Security Incident Response konfigurieren, sodass als Reaktion auf Warnmeldungen automatisierte und manuelle Aktionen in Ihrem Konto ausgeführt werden. Sie können die Eindämmung auch selbst oder in Zusammenarbeit mit Ihren Partnern durchführen, indem Sie SSM Dokumente verwenden.

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

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

- **EC2Eindämmung:** Die `AWSSupport-ContainEC2Instance` Containment-Automatisierung führt eine umkehrbare Netzwerkeindämmung einer EC2 Instance durch. Die Instance bleibt intakt und läuft, isoliert sie jedoch von jeder neuen Netzwerkaktivität und verhindert, dass sie mit Ressourcen innerhalb und außerhalb Ihrer Instanz kommuniziert. VPC


Important

Es ist wichtig zu beachten, dass bestehende nachverfolgte Verbindungen nicht aufgrund wechselnder Sicherheitsgruppen geschlossen werden. Nur future Datenverkehr wird durch die neue Sicherheitsgruppe und dieses SSM Dokument effektiv blockiert. Weitere Informationen finden Sie im Abschnitt [Source Containment](#) des technischen Leitfadens zum Service.

- **IAMEingrenzung:** Die `AWSSupport-ContainIAMPrincipal` Containment-Automatisierung führt eine umkehrbare Netzwerkbegrenzung eines IAM Benutzers oder einer Rolle durch, wobei der

Benutzer oder die Rolle zwar erhalten bleibt IAM, aber von der Kommunikation mit Ressourcen in Ihrem Konto isoliert wird.

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

 **Important**

AWS Security Incident Response aktiviert standardmäßig keine Containment-Funktionen. Um diese Eindämmungsaktionen auszuführen, müssen Sie dem Service zunächst mithilfe von Rollen die erforderlichen Berechtigungen erteilen. Sie können diese Rollen einzeln für jedes Konto oder für Ihre gesamte Organisation erstellen, indem Sie [mit AWS CloudFormation Stacksets arbeiten](#), die die erforderlichen Rollen erstellen.

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

- Mögliche Schäden an Ressourcen
 - Beweissicherung und regulatorische Anforderungen
 - Nichtverfügbarkeit von Diensten (z. B. Netzwerkkonnektivität, für externe Parteien bereitgestellte Dienste)
 - Zeit und Ressourcen, die für die Umsetzung der Strategie benötigt wurden
 - Wirksamkeit der Strategie (z. B. teilweise oder vollständige Eindämmung)
 - Dauerhaftigkeit der Lösung (z. B. reversibel oder irreversibel)
 - Dauer der Lösung (z. B. Notfalllösung, vorübergehende Behelfslösung, permanente Lösung)
- Wenden Sie Sicherheitskontrollen an, die das Risiko verringern und Zeit für die Definition und Umsetzung einer effektiveren Eindämmungsstrategie bieten.

AWS Security Incident Response empfiehlt einen schrittweisen Ansatz, um eine effiziente und effektive Eindämmung zu erreichen, der je nach Ressourcentyp kurz- und langfristige Strategien umfasst.

- Strategie zur Eindämmung
 - Kann AWS Security Incident Response den Umfang des Sicherheitsereignisses ermitteln?
 - Falls ja, identifizieren Sie alle Ressourcen (Benutzer, Systeme, Ressourcen).
 - Falls nein, untersuchen Sie dies parallel zur Ausführung des nächsten Schritts für identifizierte Ressourcen.
 - Kann die Ressource isoliert werden?
 - Falls ja, fahren Sie mit der Isolierung der betroffenen Ressourcen fort.
 - Falls nein, arbeiten Sie mit den Systembesitzern und Managern zusammen, um weitere Maßnahmen zur Eindämmung des Problems zu ergreifen.
 - Sind alle betroffenen Ressourcen von den nicht betroffenen Ressourcen isoliert?
 - Falls ja, fahren Sie mit dem nächsten Schritt fort.
 - Falls nein, sollten Sie die betroffenen Ressourcen weiter isolieren, um eine kurzfristige Eindämmung zu erreichen und eine weitere Eskalation des Ereignisses zu verhindern.
- System-Backup
 - Wurden Sicherungskopien der betroffenen Systeme zur weiteren Analyse erstellt?
 - Werden die forensischen Kopien verschlüsselt und an einem sicheren Ort gespeichert?
 - Falls ja, fahren Sie mit dem nächsten Schritt fort.
 - Falls nein, verschlüsseln Sie die forensischen Bilder und speichern Sie sie an einem sicheren Ort, um eine versehentliche Verwendung, Beschädigung und Manipulation zu verhindern.

Ausrotten

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

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

~~AWS CIRT wir prüfen gemeinsam mit Ihnen, welche Maßnahmen erforderlich sind.~~

Berücksichtigen Sie dabei Folgendes:

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

Wiederherstellung

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

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

Bericht nach dem Vorfall

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

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

Fallmetriken

- Erstellte Fälle

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

Triaging-Metriken

- Eingegangene Ergebnisse
 - Einheit: Anzahl
 - Beschreibung: Die Anzahl der Ergebnisse, die zur Prüfung gesendet wurden.
- Archivierte Ergebnisse
 - Einheit: Anzahl
 - Beschreibung: Die Anzahl der Ergebnisse, die nach der Verarbeitung ohne manuelle Untersuchung archiviert wurden.
- Manuell untersuchte Ergebnisse
 - Einheit: Anzahl
 - Beschreibung: Die Anzahl der Ergebnisse, bei denen eine manuelle Untersuchung durchgeführt wurde.
- Archivierte Untersuchungen
 - Einheit: Anzahl
 - Beschreibung: Die Anzahl der manuellen Untersuchungen, die zu Fehlalarmen geführt und zur Archivierung gesendet wurden

- Die Ermittlungen eskalierten
 - Einheit: Anzahl
 - Beschreibung: Die Anzahl der manuellen Untersuchungen, die zu einem Sicherheitsvorfall geführt haben

Fälle

AWS Mit Security Incident Response können Sie zwei Arten von Fällen erstellen: AWS unterstützte oder selbst verwaltete Fälle.

Erstellen Sie einen AWS unterstützten Fall

Sie können einen AWS unterstützten Fall aus der AWS Security Incident ResponseAPI, dem oder dem erstellen AWS Command Line Interface. AWS Unterstützte Fälle ermöglichen es Ihnen, Unterstützung vom AWS Customer Incident Response Team zu erhalten (CIRT).

Note

AWS CIRT wird innerhalb von 15 Minuten auf Ihren Fall antworten. Die Antwortzeit bezieht sich auf eine erste Antwort von AWS CIRT. Wir werden alle zumutbaren Anstrengungen unternehmen, um Ihre erste Anfrage innerhalb dieses Zeitraums zu beantworten. Diese Antwortzeit gilt nicht für nachfolgende Antworten.

Das folgende Beispiel behandelt die Verwendung der Konsole.

1. Melden Sie sich bei der an AWS Management Console. Öffnen Sie die Security Incident Response-Konsole unter <https://console.aws.amazon.com/security-ir/>.
2. Wählen Sie „Fall erstellen“
3. Wählen Sie „Fall lösen mit“ AWS
4. Wählen Sie die Art der Anfrage
 - a. Aktiver Sicherheitsvorfall: Dieser Typ ist für Support und Services zur Reaktion auf dringende Vorfälle vorgesehen.
 - b. Untersuchungen: Untersuchungen ermöglichen es Ihnen, Unterstützung bei festgestellten Sicherheitsvorfällen zu erhalten, indem sie die Untersuchung protokollieren und die Untersuchung der Reaktion auf Sicherheitsvorfälle sekundär bestätigen AWS CIRT können.

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

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

Nachdem ein AWS unterstützter Fall erstellt wurde, werden das Incident-Response-Team AWS CIRT und Ihr Incident-Response-Team sofort benachrichtigt.

Erstellen Sie einen selbst verwalteten Fall

Sie können aus der AWS Security Incident Response, dem oder dem API einen selbstverwalteten erstellen. AWS Command Line Interface Bei dieser Art von Fall handelt es DOESNOTsich um die AWS CIRT. Das folgende Beispiel behandelt die Verwendung der Konsole.

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

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

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

Auf einen AWS generierten Fall antworten

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

Diese Benachrichtigungen werden in der Support Mitte angezeigt. Das Support Benutzerhandbuch enthält Informationen und detaillierte Schritte zur [Aktualisierung, Lösung und erneuten Eröffnung dieser Fälle](#).

Fälle verwalten

Inhalt

- [Den Fallstatus ändern](#)
- [Den Resolver ändern](#)
- [Aktionselemente](#)
- [Bearbeiten eines Falls](#)
- [Kommunikation](#)
- [Berechtigungen](#)
- [Anlagen](#)
- [Tags](#)
- [Fallaktivitäten](#)
- [Einen Fall schließen](#)

Den Fallstatus ändern

Ein Fall wird sich in einem der folgenden Staaten befinden:

- **Eingereicht:** Dies ist der ursprüngliche Status eines Falls. Fälle in diesem Status wurden von einer angefragten Person eingereicht, werden aber noch nicht bearbeitet.
- **Erkennung und Analyse:** Dieser Status zeigt an, dass ein Incident-Responder mit der Bearbeitung des Falls begonnen hat. Diese Phase umfasst die Erfassung von Daten, die Einstufung des Ereignisses und die Durchführung von Analysen, um datengestützte Schlussfolgerungen zu ziehen.
- **Eindämmung, Beseitigung und Wiederherstellung:** In diesem Status hat der Incident Responder verdächtige Aktivitäten identifiziert, deren Beseitigung zusätzlichen Aufwand erfordert. Der Incident Responder gibt Ihnen Empfehlungen für die Analyse des Geschäftsrisikos und weitere Maßnahmen. Wenn Sie die Opt-in-Funktionen für den Service aktiviert haben, wird ein AWS Incident Responder Sie um Ihre Zustimmung bitten, Eindämmungsmaßnahmen mit SSM Dokumenten in den betroffenen Konten durchzuführen.
- **Aktivitäten nach dem Vorfall:** In diesem Status wurde das primäre Sicherheitsereignis eingedämmt. Der Schwerpunkt liegt nun auf der Wiederherstellung und Wiederherstellung des normalen Geschäftsbetriebs. Wenn der Resolver für den Fall unterstützt wird, werden eine Zusammenfassung und eine AWS Ursachenanalyse bereitgestellt.
- **Geschlossen:** Dies ist der endgültige Status des Workflows. Fälle mit dem Status „Abgeschlossen“ weisen darauf hin, dass die Arbeit abgeschlossen wurde. Geschlossene Fälle können nicht erneut

geöffnet werden. Stellen Sie daher sicher, dass alle Aktionen abgeschlossen sind, bevor Sie zu diesem Status wechseln.

Wählen Sie Aktion/Status aktualisieren, um den Status des Falls für selbst verwaltete Fälle zu ändern. Bei AWS unterstützten Fällen wird der Status vom Responder festgelegt. AWS CIRT

Den Resolver ändern

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

Aktionselemente

Ein AWS CIRT Responder, der an dem Fall arbeitet, kann Ihr internes Team um Maßnahmen bitten.

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

- Bitte um Erteilung von Zugriffsberechtigungen für einen Incident-Responder für den Zugriff auf einen Fall
- Bitte um weitere Informationen zu dem Fall

Aktionspunkt, wenn eine Kundenaktion aussteht:

- Bitte um Bearbeitung eines neuen Kommentars, um den Fall weiter bearbeiten zu können

Aktionspunkte, wenn ein Fall zum Abschluss bereit ist:

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

Bearbeiten eines Falls

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

Für AWS unterstützte und selbst verwaltete Fälle:

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

- Title
- Beschreibung

Nur für AWS unterstützte Fälle:

Sie können die zusätzlichen Felder ändern:

- Art der Anfrage:
 - Aktiver Sicherheitsvorfall: Bei diesem Typ handelt es sich um Support und Services zur Reaktion auf dringende Vorfälle.
 - Untersuchungen: Untersuchungen ermöglichen es Ihnen, Unterstützung bei festgestellten Sicherheitsvorfällen zu erhalten. Dabei AWS CIRT können wir Ihnen eine Protokollaufnahme und eine sekundäre Bestätigung der Untersuchung des Vorfalls zur Verfügung stellen.
- Voraussichtliches Startdatum: Ändern Sie dieses Feld, wenn Sie für diesen Fall Indikatoren erhalten haben, die vor dem ursprünglich angegebenen Startdatum liegen. Erwägen Sie, zusätzliche Details zu dem neu erkannten Indikator im Beschreibungsfeld anzugeben oder auf der Registerkarte Kommunikation einen Kommentar hinzuzufügen.

Kommunikation

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

Berechtigungen

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

Note

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

Gewähren Sie Zugriff auf einen Fall in der Konsole

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

Hinzufügen der IAM Richtlinie zu einem Benutzer oder einer Rolle:

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

Anlagen

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

Note

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

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

Note

Alle hochgeladenen Anlagen werden sieben Tage nach Abschluss eines Falls gelöscht.

Tags

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

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

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

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

Fallaktivitäten

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

Einen Fall schließen

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

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

Note

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

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

Mit AWS CloudFormation Stacksets arbeiten

Important

AWS Security Incident Response aktiviert standardmäßig keine Containment-Funktionen. Um diese Eindämmungsaktionen auszuführen, müssen Sie dem Service zunächst mithilfe von Rollen die erforderlichen Berechtigungen erteilen. Sie können diese Rollen einzeln pro Konto oder unternehmensweit erstellen, indem Sie sie bereitstellen AWS CloudFormation StackSets, wodurch die erforderlichen Rollen erstellt werden.

Sie finden spezifische Anweisungen zum [Erstellen eines Stack-Sets mit vom Service verwalteten Berechtigungen](#).

Im Folgenden finden Sie Vorlagen-Stacksets zum Erstellen der `AWSecurityIncidentResponseContainmentRoles` und `AWSecurityIncidentResponseContainmentExecution`

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for AWS Security Incident Response containment roles'

Resources:
  AWSecurityIncidentResponseContainment:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSecurityIncidentResponseContainment
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:AssumeRole',
```

```

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

```

```

    },
  ],
}
AWSSecurityIncidentResponseContainmentExecution:
  Type: 'AWS::IAM::Role'
  Properties:
    RoleName: AWSSecurityIncidentResponseContainmentExecution
    AssumeRolePolicyDocument:
      {
        'Version': '2012-10-17',
        'Statement':
          [{ 'Effect': 'Allow', 'Principal': { 'Service': 'ssm.amazonaws.com' } },
'Action': 'sts:AssumeRole' ]],
      }
    ManagedPolicyArns:
      - !Sub arn:${AWS::Partition}:iam::aws:policy/SecurityAudit
    Policies:
      - PolicyName: AWSSecurityIncidentResponseContainmentExecutionPolicy
        PolicyDocument:
          {
            'Version': '2012-10-17',
            'Statement':
              [
                {
                  'Sid': 'AllowIAMContainment',
                  'Effect': 'Allow',
                  'Action':
                    [
                      'iam:AttachRolePolicy',
                      'iam:AttachUserPolicy',
                      'iam:DeactivateMFADevice',
                      'iam>DeleteLoginProfile',
                      'iam>DeleteRolePolicy',
                      'iam>DeleteUserPolicy',
                      'iam:GetLoginProfile',
                      'iam:GetPolicy',
                      'iam:GetRole',
                      'iam:GetRolePolicy',
                      'iam:GetUser',
                      'iam:GetUserPolicy',
                      'iam>ListAccessKeys',
                      'iam>ListAttachedRolePolicies',
                      'iam>ListAttachedUserPolicies',
                      'iam>ListMfaDevices',

```

```
        'iam:ListPolicies',
        'iam:ListRolePolicies',
        'iam:ListUserPolicies',
        'iam:ListVirtualMFADevices',
        'iam:PutRolePolicy',
        'iam:PutUserPolicy',
        'iam:TagMFADevice',
        'iam:TagPolicy',
        'iam:TagRole',
        'iam:TagUser',
        'iam:UntagMFADevice',
        'iam:UntagPolicy',
        'iam:UntagRole',
        'iam:UntagUser',
        'iam:UpdateAccessKey',
        'identitystore:CreateGroupMembership',
        'identitystore>DeleteGroupMembership',
        'identitystore:IsMemberInGroups',
        'identitystore:ListUsers',
        'identitystore:ListGroups',
        'identitystore:ListGroupMemberships',
    ],
    'Resource': '*',
  },
  {
    'Sid': 'AllowOrgListAccounts',
    'Effect': 'Allow',
    'Action': 'organizations:ListAccounts',
    'Resource': '*',
  },
  {
    'Sid': 'AllowSSOContainment',
    'Effect': 'Allow',
    'Action':
      [
        'sso:CreateAccountAssignment',
        'sso>DeleteAccountAssignment',
        'sso>DeleteInlinePolicyFromPermissionSet',
        'sso:GetInlinePolicyForPermissionSet',
        'sso:ListAccountAssignments',
        'sso:ListInstances',
        'sso:ListPermissionSets',
        'sso:ListPermissionSetsProvisionedToAccount',
        'sso:PutInlinePolicyToPermissionSet',
```



```
        'sso:TagResource',
        'sso:UntagResource',
    ],
    'Resource': '*',
},
{
    'Sid': 'AllowSSORead',
    'Effect': 'Allow',
    'Action': ['sso-directory:SearchUsers', 'sso-
directory:DescribeUser'],
    'Resource': '*',
},
{
    'Sid': 'AllowS3Read',
    'Effect': 'Allow',
    'Action':
    [
        's3:GetAccountPublicAccessBlock',
        's3:GetBucketAcl',
        's3:GetBucketLocation',
        's3:GetBucketOwnershipControls',
        's3:GetBucketPolicy',
        's3:GetBucketPolicyStatus',
        's3:GetBucketPublicAccessBlock',
        's3:GetBucketTagging',
        's3:GetEncryptionConfiguration',
        's3:GetObject',
        's3:GetObjectAcl',
        's3:GetObjectTagging',
        's3:GetReplicationConfiguration',
        's3:ListBucket',
        's3express:GetBucketPolicy',
    ],
    'Resource': '*',
},
{
    'Sid': 'AllowS3Write',
    'Effect': 'Allow',
    'Action':
    [
        's3:CreateBucket',
        's3>DeleteBucketPolicy',
        's3>DeleteObjectTagging',
        's3:PutAccountPublicAccessBlock',
```

```
        's3:PutBucketACL',
        's3:PutBucketOwnershipControls',
        's3:PutBucketPolicy',
        's3:PutBucketPublicAccessBlock',
        's3:PutBucketTagging',
        's3:PutBucketVersioning',
        's3:PutObject',
        's3:PutObjectAcl',
        's3express:CreateSession',
        's3express>DeleteBucketPolicy',
        's3express:PutBucketPolicy',
    ],
    'Resource': '*',
},
{
    'Sid': 'AllowAutoScalingWrite',
    'Effect': 'Allow',
    'Action':
        [
            'autoscaling:CreateOrUpdateTags',
            'autoscaling>DeleteTags',
            'autoscaling:DescribeAutoScalingGroups',
            'autoscaling:DescribeAutoScalingInstances',
            'autoscaling:DescribeTags',
            'autoscaling:EnterStandby',
            'autoscaling:ExitStandby',
            'autoscaling:UpdateAutoScalingGroup',
        ],
    'Resource': '*',
},
{
    'Sid': 'AllowEC2Containment',
    'Effect': 'Allow',
    'Action':
        [
            'ec2:AuthorizeSecurityGroupEgress',
            'ec2:AuthorizeSecurityGroupIngress',
            'ec2:CopyImage',
            'ec2:CreateImage',
            'ec2:CreateSecurityGroup',
            'ec2:CreateSnapshot',
            'ec2:CreateTags',
            'ec2>DeleteSecurityGroup',
            'ec2>DeleteTags',
```

```

        'ec2:DescribeImages',
        'ec2:DescribeInstances',
        'ec2:DescribeSecurityGroups',
        'ec2:DescribeSnapshots',
        'ec2:DescribeTags',
        'ec2:ModifyNetworkInterfaceAttribute',
        'ec2:RevokeSecurityGroupEgress',
    ],
    'Resource': '*',
},
{
    'Sid': 'AllowKMSActions',
    'Effect': 'Allow',
    'Action':
        [
            'kms:CreateGrant',
            'kms:DescribeKey',
            'kms:GenerateDataKeyWithoutPlaintext',
            'kms:ReEncryptFrom',
            'kms:ReEncryptTo',
        ],
    'Resource': '*',
},
{
    'Sid': 'AllowSSMActions',
    'Effect': 'Allow',
    'Action': ['ssm:DescribeAutomationExecutions'],
    'Resource': '*',
},
],
}


```

Mitgliedschaft kündigen

Eine Rolle, die über die CancelMembership Berechtigung zur Reaktion auf AWS Sicherheitsvorfälle verfügt, kann die Mitgliedschaft über die KonsoleAPI, die oder kündigen AWS Command Line Interface.

 **Important**

Sobald eine Mitgliedschaft gekündigt wurde, können Sie keine historischen Falldaten mehr einsehen. Kündigungen erfolgen am Ende des Abrechnungszeitraums. Wenn Sie im Laufe des Monats kündigen, ist Ihre Mitgliedschaft bis Ende des Monats verfügbar. Alle Ressourcen oder Untersuchungen, die nach der endgültigen Kündigung der Mitgliedschaft am Ende des Abrechnungszeitraums eingestellt sind `Active` oder `ready to close` werden.

 **Important**

Wenn Sie den Service erneut abonnieren, wird eine neue Mitgliedschaft erstellt und die Fallressourcen, die im Rahmen der vorherigen Mitgliedschaft verfügbar waren, sind nur verfügbar, wenn Sie sie vor der Kündigung heruntergeladen haben.

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

 **Important**

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

Ressourcen zur Reaktion auf AWS Sicherheitsvorfälle kennzeichnen

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

Tags sind für folgende Aktivitäten nützlich:

- Identifizieren und organisieren Sie Ihre AWS Ressourcen. Viele AWS-Services unterstützen Tagging, sodass Sie Ressourcen aus verschiedenen Diensten dasselbe Tag zuweisen können, um anzuzeigen, dass die Ressourcen miteinander verknüpft sind.
- Verfolgen Sie Ihre AWS Kosten. Sie aktivieren diese Tags auf dem AWS Billing Dashboard. AWS verwendet die Tags, um Ihre Kosten zu kategorisieren und Ihnen einen monatlichen Kostenverteilungsbericht zu senden. Weitere Informationen finden Sie im [AWS Billing User Guide](#) unter [Verwenden von Tags für die Kostenzuweisung](#).
- Steuern Sie den Zugriff auf Ihre AWS Ressourcen. Weitere Informationen finden Sie im [IAMBenutzerhandbuch](#) unter [Steuern des Zugriffs mithilfe von Tags](#).

Informationen zur [Kennzeichnung finden Sie in der API Referenz zur Reaktion auf AWS Sicherheitsvorfälle](#).

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

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

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

Inhalt

- [Erlangung von Berechtigungen für IAM AWS CloudShell](#)
- [Interaktion mit Security Incident Response mithilfe von AWS CloudShell](#)

Erlangung von Berechtigungen für IAM AWS CloudShell


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

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

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

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


AWS CloudShell FullAccess verwaltete Richtlinie als Vorlage verwendet. Weitere Informationen zur Einschränkung der Aktionen, die Benutzern zur Verfügung stehen CloudShell, finden Sie im AWS CloudShell Benutzerhandbuch unter [AWS CloudShell Zugriff und Nutzung mithilfe von IAM Richtlinien verwalten](#).

 Note

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

Interaktion mit Security Incident Response mithilfe von AWS CloudShell

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

 Note

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

Arbeit mit Sicherheitsvorfällen AWS CloudShell und Reaktion auf Sicherheitsvorfälle

- Von der aus können Sie starten AWS Management Console, CloudShell indem Sie die folgenden Optionen auswählen, die in der Navigationsleiste verfügbar sind:
 - Wählen Sie das CloudShell Symbol.
 - Geben Sie „Cloudshell“ in das Suchfeld ein und wählen Sie dann die CloudShell Option.

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

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

Weitere Informationen CloudTrail dazu finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

Informationen zur Reaktion auf Sicherheitsvorfälle finden Sie unter CloudTrail

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

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

CloudTrail Pfade

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

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

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

CloudTrail Datenspeicher für Ereignisse in Lake

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

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

Alle Maßnahmen zur Reaktion auf Sicherheitsvorfälle werden von der [AWS Security Incident Response API Reference](#) protokolliert CloudTrail und sind in dieser dokumentiert. Beispielsweise generieren Aufrufe von CreateCase und UpdateCase Aktionen Einträge in den CloudTrail Protokolldateien. CreateMembership

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

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

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

Weitere Informationen finden Sie im [CloudTrail userIdentityElement](#).

Die Einträge der Security Incident Response-Protokolldatei verstehen

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

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

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAA00000000000000000000000000000000:user",
    "arn": "arn:aws:sts::123412341234:assumed-role/Admin/user",
    "accountId": "123412341234",
    "accessKeyId": "*****",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAA00000000000000000000000000000000",
        "arn": "arn:aws:iam::123412341234:role/Admin",
        "accountId": "123412341234",
        "userName": "Admin"
      },
      "attributes": {
        "creationDate": "2024-10-13T06:32:53Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2024-10-13T06:40:45Z",
  "eventSource": "security-ir.amazonaws.com",
```

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

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

Verwaltung von AWS Security Incident Response-Konten mit AWS Organizations

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

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

Inhalt

- [Überlegungen und Empfehlungen zur Verwendung von AWS Security Incident Response mit AWS Organizations](#)
- [Aktivierung des vertrauenswürdigen Zugriffs für AWS Account Management](#)
- [Für die Benennung eines delegierten Security Incident Response-Administratorkontos sind Berechtigungen erforderlich](#)
- [Benennen Sie einen delegierten Administrator für Security Incident Response AWS](#)
- [Mitglieder zu AWS Security Incident Response hinzufügen](#)
- [Mitglieder aus AWS Security Incident Response entfernen](#)

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

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

Ein delegiertes Security Incident Response-Administratorkonto ist regional.

Das delegierte Security Incident Response-Administratorkonto und die Mitgliedskonten müssen über hinzugefügt werden. AWS Organizations

Delegiertes Administratorkonto für AWS Security Incident Response.

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

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

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

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

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

Aktivierung des vertrauenswürdigen Zugriffs für AWS Account Management

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

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

Mindestberechtigungen

Um diese Aufgaben ausführen zu können, müssen Sie die folgenden Anforderungen erfüllen:

- Sie können dies nur über das Verwaltungskonto der Organisation ausführen.
- Für Ihre Organisation müssen [alle Funktionen aktiviert sein](#).

Console

Um vertrauenswürdigen Zugriff für AWS Security Incident Response zu aktivieren

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

API/CLI

Um vertrauenswürdigen Zugriff zu aktivieren für AWS Account Management

Nachdem Sie den folgenden Befehl ausgeführt haben, können Sie die Anmeldeinformationen des Verwaltungskontos der Organisation verwenden, um API Kontoverwaltungsvorgänge aufzurufen, die den `--accountId` Parameter verwenden, um auf Mitgliedskonten in einer Organisation zu verweisen.

- AWS CLI: [enable-aws-service-access](#)

Das folgende Beispiel ermöglicht den vertrauenswürdigen Zugriff für AWS Security Incident Response in der Organisation des anrufenden Accounts.

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

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

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

Sie können wählen, ob Sie Ihre AWS Security Incident Response-Mitgliedschaft mit delegiertem Administrator für einrichten möchten. AWS Organizations Informationen darüber, wie diese Berechtigungen gewährt werden, finden Sie unter Zusammen [AWS Organizations mit anderen AWS Diensten verwenden](#).

Note

AWS Security Incident Response aktiviert automatisch die AWS Organizations Vertrauensbeziehung, wenn die Konsole für die Einrichtung und Verwaltung verwendet wird. Wenn Sie CLI verwenden, müssen Sie SDK dies manuell aktivieren, indem Sie den [Enable AWS Service Access API to Trust](#) verwenden `security-ir.amazonaws.com`.

Bevor Sie als AWS Organizations Manager das delegierte Security Incident Response-Administratorkonto für Ihr Unternehmen festlegen, stellen Sie sicher, dass Sie die folgenden AWS Security Incident Response-Aktionen ausführen können: `sir:CreateMembership` und `sir:UpdateMembership`. Diese Aktionen ermöglichen es Ihnen, mithilfe von AWS Security Incident Response das delegierte Security Incident Response-Administratorkonto für Ihr Unternehmen festzulegen. Sie müssen außerdem sicherstellen, dass Sie die AWS Organizations Aktionen ausführen dürfen, mit denen Sie Informationen über Ihre Organisation abrufen können.

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

```
{
  "Sid": "PermissionsForSIRAdmin",
  "Effect": "Allow",
  "Action": [
    "security-ir:CreateMembership",
    "security-ir:UpdateMembership",
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
```



```

    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource": "*"
}

```

Wenn Sie Ihr AWS Organizations Management als delegiertes Security Incident Response-Administratorkonto festlegen möchten, benötigt Ihr Konto auch die folgende IAM Aktion: `CreateServiceLinkedRole`. Mit dieser Aktion können Sie AWS Security Incident Response für das Management initialisieren. Überprüfen Sie dies jedoch, [Überlegungen und Empfehlungen zur Verwendung von AWS Security Incident Response mit AWS Organizations](#) bevor Sie die Berechtigungen hinzufügen.

Um die Verwaltung weiterhin als delegiertes Security Incident Response-Administratorkonto festzulegen, fügen Sie der IAM Richtlinie die folgende Erklärung hinzu und `111122223333` ersetzen Sie sie durch die AWS-Konto ID der Geschäftsleitung Ihrer Organisation:

```

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

```

Benennen Sie einen delegierten Administrator für Security Incident Response AWS

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

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

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

Console

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

Um sich anzumelden, verwenden Sie die Verwaltungsdaten Ihrer AWS Organizations Organisation.

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

API/CLI

- Führen Sie die Ausführung `CreateMembership` mit den Anmeldeinformationen AWS-Konto des Managements der Organisation aus.
- Alternativ können Sie AWS Command Line Interface dies verwenden. Der folgende AWS CLI Befehl bestimmt ein delegiertes Security Incident Response-Administratorkonto. Im Folgenden sind die Zeichenkettenoptionen aufgeführt, die für die Konfiguration Ihrer Mitgliedschaft verfügbar sind:

```
{
  "customerAccountId": "stringstring",
  "membershipName": "stringstring",
  "customerType": "Standalone",
  "organizationMetadata": {
    "organizationId": "string",
```

```

    "managementAccountId": "stringstring",
    "delegatedAdministrators": [
      "stringstring"
    ]
  },
  "membershipAccountsConfigurations": {
    "autoEnableAllAccounts": true,
    "organizationalUnits": [
      "string"
    ]
  },
  "incidentResponseTeam": [
    {
      "name": "string",
      "jobTitle": "stringstring",
      "email": "stringstring"
    }
  ],
  "internalIdentifier": "string",
  "membershipId": "stringstring",
  "optInFeatures": [
    {
      "featureName": "RuleForwarding",
      "isEnabled": true
    }
  ]
}

```

Wenn AWS Security Incident Response für Ihr delegiertes Security Incident Response-Administratorkonto nicht aktiviert ist, kann es keine Maßnahmen ergreifen. Falls dies noch nicht geschehen ist, stellen Sie sicher, dass AWS Security Incident Response für das neu benannte delegierte Security Incident Response-Administratorkonto aktiviert ist.

Mitglieder zu AWS Security Incident Response hinzufügen

Es besteht eine persönliche Beziehung mit AWS Organizations und Ihrer Mitgliedschaft bei AWS Security Incident Response. Wenn Konten zu Ihren Organizations hinzugefügt (oder entfernt) werden, spiegelt sich dies in den abgedeckten Konten für Ihre Mitgliedschaft bei AWS Security Incident Response wider.

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

Mitglieder aus AWS Security Incident Response entfernen

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

Fehlerbehebung

Wenn Sie Probleme im Zusammenhang mit der Durchführung einer spezifischen Aktion für die Reaktion auf AWS Sicherheitsvorfälle haben, lesen Sie die Themen in diesem Abschnitt.

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

Inhalt

- [Problembereiche](#)
- [Fehler](#)
- [Support](#)

Problembereiche

Anfragen werden nicht aus dem richtigen Kontext gesendet.

Alle Anrufe an AWS Security Incident Response APIs müssen von einem IAM Principal im Service stammen, dem ein Administrator- oder Mitgliedskonto zugewiesen wurde. Stellen Sie sicher, dass Sie mit dem richtigen IAM Principal arbeiten, das ist AWS-Konto das delegierte Administrator- oder Mitgliedskonto Ihrer Organisation für AWS Security Incident Response.

Fehler

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

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

ConflictException

Die Anfrage verursacht einen inkonsistenten Status.

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

InternalServerErrorException

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

ResourceNotFoundException

Die Anfrage verweist auf eine Ressource, die nicht existiert.

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

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

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

ValidationException

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

Eines oder mehrere der Datenfelder in Ihrer Anfrage erfüllten nicht die Validierungs- und/oder logischen Kombinationsanforderungen. Bitte überprüfen Sie, ob alle Ressourcen ARNs vollständig sind und ob die Textwerte die Größen- und Formatbeschränkungen aus dem [AWS Security Incident Response API Reference Guide](#) erfüllen. Vergewissern Sie sich auch, dass Wertaktualisierungen zulässig sind. Es ist beispielsweise nicht möglich, einen Fall von „AWS unterstützt“ in „Selbstverwaltet“ zu ändern.

Support

Wenn Sie zusätzliche Unterstützung benötigen, wenden Sie sich zur Problembeseitigung an das [Support Center](#). Halten Sie bitte die folgenden Informationen bereit:

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

Sicherheit

Inhalt

- [Datenschutz bei der Reaktion auf AWS Sicherheitsvorfälle](#)
- [Datenschutz für den Datenverkehr zwischen Netzwerken](#)
- [Identitäts- und Zugriffsverwaltung](#)
- [Behebung von AWS Sicherheitsvorfällen, Identität und Zugriff](#)
- [Verwenden von Servicerollen](#)
- [Verwenden von serviceverknüpften Rollen](#)
- [AWS Verwaltete Richtlinien](#)
- [Vorfallreaktion](#)
- [Compliance-Validierung](#)
- [Protokollierung und Überwachung in AWS Security Incident Response](#)
- [Ausfallsicherheit](#)
- [Sicherheit der Infrastruktur](#)
- [Konfigurations- und Schwachstellenanalyse](#)
- [Serviceübergreifende Confused-Deputy-Prävention](#)

Datenschutz bei der Reaktion auf AWS Sicherheitsvorfälle

Inhalt

- [Datenverschlüsselung](#)

Das [Modell der AWS gemeinsamen Verantwortung](#) gilt für den Datenschutz im Rahmen des AWS Security Incident Response-Service. AWS ist, wie in diesem Modell beschrieben, für den Schutz der Infrastruktur verantwortlich, auf der die in der AWS Cloud angebotenen Dienste ausgeführt werden. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben der von Ihnen verwendeten AWS Dienste verantwortlich. Weitere Informationen zum Datenschutz finden Sie im [Datenschutz FAQ](#). Informationen zum Datenschutz in Europa finden Sie im [AWS Shared Responsibility Model und](#) im GDPR Blogbeitrag auf dem AWS Security Blog.

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

- Verwenden Sie für jedes Konto eine Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen innerhalb der AWS Dienste.
- FIPS140-3 wird derzeit vom Dienst nicht unterstützt.

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

Datenverschlüsselung

Inhalt

- [Verschlüsselung im Ruhezustand](#)
- [Verschlüsselung während der Übertragung](#)
- [Schlüsselverwaltung](#)

Verschlüsselung im Ruhezustand

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

Verschlüsselung während der Übertragung

Die von AWS Security Incident Response gesammelten und abgerufenen Daten werden ausschließlich über einen durch Transport Layer Security (TLS) geschützten Kanal übertragen.

Schlüsselverwaltung

AWS Security Incident Response implementiert Integrationen AWS KMS zur Verschlüsselung von Fall- und Anhangsdaten im Ruhezustand.

AWS Security Incident Response unterstützt keine vom Kunden verwalteten Schlüssel.

Datenschutz für den Datenverkehr zwischen Netzwerken

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

Sie haben zwei Verbindungsoptionen zwischen Ihrem privaten Netzwerk und AWS:


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

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

Datenverkehr zwischen AWS -Ressourcen in derselben Region

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

Antworten zurück an die VPC. Weitere Informationen finden Sie unter [VPC Endpoints](#) im VPC Amazon-Benutzerhandbuch. Richtlinien, mit denen Sie den Zugriff von VPC Endpunkten aus steuern können, finden Sie beispielsweise unter [Verwenden von IAM Richtlinien zur Steuerung des Zugriffs auf DynamoDB](#).

 Note

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

Identitäts- und Zugriffsverwaltung

AWS Identity and Access Management (IAM) ist ein AWS Dienst, der einem Administrator hilft, den Zugriff auf AWS Ressourcen zu kontrollieren. IAM Administratoren kontrollieren authentifizierte (angemeldete) und autorisierte (mit Berechtigungen) Prinzipale, die Ressourcen zur Reaktion auf AWS Sicherheitsvorfälle nutzen können. IAM ist ein AWS Service, den Sie ohne zusätzliche Kosten nutzen können.

Inhalt

- [Authentifizierung mit Identitäten](#)
- [So funktioniert die Reaktion auf AWS Sicherheitsvorfälle mit IAM](#)

Publikum

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in AWS Security Incident Response ausführen.

Sicherheitsadministratoren

Diesen Benutzern wird empfohlen, die [AWS Security Incident Response Full Access](#) verwaltete Richtlinie zu verwenden, um sicherzustellen, dass sie Lese- und Schreibzugriff auf Mitgliedschafts- und Fallressourcen haben.

Fallbeobachter

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

Mitglieder des Incident Response Teams

Mitgliedern des Teams können sowohl Vollmitgliedschaft als auch Zugang zu Fällen gewährt werden. Es wird empfohlen, dass nicht alle Personen über verbindliche Maßnahmen zur Mitgliedschaft im Dienst verfügen, sondern dass sie Zugriff auf alle Fälle haben, die über den Dienst erstellt und verwaltet werden. Weitere Informationen finden Sie unter [Verwaltete Richtlinien zur Reaktion auf AWS Sicherheitsvorfälle](#).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als Root-Benutzer des AWS Kontos, als Benutzer oder durch Übernahme einer IAM IAM Rolle authentifiziert (angemeldet AWS) sein.

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) - Nutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

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

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

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter [Multi-Faktor-Authentifizierung](#) im AWS IAM Identity Center-Benutzerhandbuch und [Verwenden der Multi-Faktor-Authentifizierung \(MFA\) AWS im IAM Benutzerhandbuch](#).

AWS Konto (Root-Benutzer)

Wenn Sie ein AWS Konto erstellen, beginnen Sie mit einer einzigen Anmeldeidentität, die vollständigen Zugriff auf alle AWS Dienste und Ressourcen im Konto hat. Diese Identität wird als Root-Benutzer des AWS Kontos bezeichnet. Sie können darauf zugreifen, indem Sie sich mit den 8 Adressen und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Verwenden Sie den Root-Benutzer niemals für Ihre täglichen Aufgaben und ergreifen Sie Maßnahmen, um Ihre Root-Benutzeranmeldedaten zu schützen. Verwenden Sie sie nur, um Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie im Benutzerhandbuch unter [Aufgaben, für die Root-Benutzeranmeldedaten erforderlich](#) sind. IAM

Föderierte Identität

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

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

Für eine zentralisierte Zugriffsverwaltung empfehlen wir die Verwendung von AWS IAM Identity Center. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie für alle Ihre AWS Konten und Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter [Was ist IAM Identity Center?](#) im AWS IAM Identity Center-Benutzerhandbuch.

IAM Benutzer und Gruppen

Ein [IAM Benutzer](#) ist eine Identität in Ihrem AWS Konto, die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie einen bestimmten Anwendungsfall haben, für den langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich](#) sind.

Eine IAM [Gruppe](#) ist eine Identität, die eine Sammlung von IAM Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdmins und dieser Gruppe Berechtigungen zur Verwaltung von IAM Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter [Wann sollte ein IAM Benutzer \(statt einer Rolle\) erstellt werden?](#) im IAM Benutzerhandbuch.

IAM -Rollen

Eine IAM [Rolle](#) ist eine Identität innerhalb Ihres AWS Kontos, die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM Rolle in der AWS Management Console übernehmen, indem Sie die [Rollen wechseln](#). Sie können eine Rolle übernehmen, indem Sie eine AWS CLI AWS API OR-Operation aufrufen oder eine benutzerdefinierte Operation verwenden URL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie [unter Verwenden von IAM Rollen](#) im IAM Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- **Föderierter Benutzerzugriff** — Um einer föderierten Identität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie im IAM Benutzerhandbuch unter [Erstellen einer Rolle für einen externen Identitätsanbieter](#). Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in. IAM Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze](#) im AWS IAM Identity Center-Benutzerhandbuch.
- **Temporäre IAM Benutzerberechtigungen** — Ein IAM Benutzer oder eine Rolle kann eine IAM Rolle übernehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- **Kontoübergreifender Zugriff** — Sie können eine IAM Rolle verwenden, um jemandem (einem vertrauenswürdigen Principal) in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu

gewähren. Bei einigen AWS Diensten können Sie jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie [IAM Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff](#). IAM

- **Serviceübergreifender Zugriff** — Einige AWS Dienste verwenden Funktionen in anderen Diensten. AWS Wenn Sie beispielsweise einen Service aufrufen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
 - **Servicerolle** — Eine Servicerolle ist eine [IAMRolle](#), die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS -Service](#) im IAM-Benutzerhandbuch.
 - **Dienstbezogene Rolle** — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einem AWS Dienst verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen werden in Ihrem AWS Konto angezeigt und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.
- **Auf Amazon ausgeführte Anwendungen EC2** — Sie können eine IAM Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API Anfragen stellen AWS CLI. Das ist empfehlenswerter, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2 Instance eine AWS Rolle zuzuweisen und sie ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [Verwenden einer IAM Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden](#).

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden [Sie im Benutzerhandbuch unter Wann sollte eine IAM Rolle \(anstelle eines IAM Benutzers\) erstellt werden](#).

So funktioniert die Reaktion auf AWS Sicherheitsvorfälle mit IAM

AWS Identity and Access Management (IAM) ist ein AWS Dienst, der einem Administrator hilft, den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAMAdministratoren kontrollieren, wer

authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zur Reaktion auf AWS Sicherheitsvorfälle zu nutzen. IAM ist ein AWS Service, den Sie ohne zusätzliche Kosten nutzen können.

IAM-Funktionen, die Sie mit AWS Security Incident Response verwenden können	
<u>IAM-Funktion</u>	<u>Ausrichtung der Dienste</u>
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Schlüssel zu den politischen Bedingungen	Ja (global)
ACLs	Nein
ABAC (Markierungen in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Zugriffssitzungen weiterleiten () FAS	Ja
Service-Rollen	Nein
Serviceverknüpfte Rollen	Ja

Inhalt

- [Identitätsbasierte Richtlinien für die Reaktion auf Sicherheitsvorfälle AWS](#)

Identitätsbasierte Richtlinien für die Reaktion auf Sicherheitsvorfälle AWS

Identitätsbasierte Richtlinien sind Dokumente mit JSON-Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM-Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und

unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter [IAMRichtlinien erstellen im Benutzerhandbuch](#). IAM

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden können, finden Sie im IAMBenutzerhandbuch unter [Referenz zu IAM JSON Richtlinienelementen](#).

Inhalt

- [Beispiele für identitätsbasierte Richtlinien](#)
- [Bewährte Methoden für Richtlinien](#)
- [Verwenden der AWS Security Incident Response-Konsole](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)
- [Schlüssel zu den Richtlinienbedingungen für die Reaktion auf AWS Sicherheitsvorfälle](#)
- [Zugriffskontrolllisten \(ACLs\) in AWS Security Incident Response](#)

Beispiele für identitätsbasierte Richtlinien

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Ressourcen zur Reaktion auf AWS Sicherheitsvorfälle zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Managementkonsole, der AWS Befehlszeilenschnittstelle (AWS CLI) oder ausführen AWS API. Ein IAM Administrator kann IAM Richtlinien erstellen, um Benutzern die Erlaubnis zu erteilen, Aktionen mit den benötigten Ressourcen durchzuführen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter [IAMRichtlinien erstellen](#) im IAMBenutzerhandbuch.

Einzelheiten zu den Aktionen und Ressourcentypen, die von AWS Security Incident Response definiert werden, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Security Incident Response in der Service Authorization Reference.

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Ressourcen zur Reaktion auf AWS Sicherheitsvorfälle in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Diese Aktionen können mit Kosten für Ihr Konto verbunden sein. AWS Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem Konto verfügbar. AWS Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie AWS im IAMBenutzerhandbuch unter [AWS Verwaltete Richtlinien oder Verwaltete Richtlinien für Jobfunktionen](#).

Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung IAM zum Anwenden von Berechtigungen finden Sie [IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen](#). IAM

Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen mit gesendet werden müssenSSL. Sie können Bedingungen auch verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten AWS Dienst verwendet werden, z. AWS CloudFormation B. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [IAMJSONRichtlinienelemente: Bedingung](#).

Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtlinien Sprache (JSON) und den IAM bewährten Methoden entsprechen. IAM Access Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter [IAMAccess Analyzer-Richtlinienvvalidierung](#) im IAMBenutzerhandbuch.

Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, das IAM Benutzer oder einen Root-Benutzer in Ihrem AWS Konto erfordert, aktivieren Sie die Option MFA für zusätzliche Sicherheit. Wenn Sie festlegen möchten, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter [Konfiguration des MFA -geschützten API Zugriffs](#) im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter [Bewährte Sicherheitsmethoden IAM im IAM](#) Benutzerhandbuch. IAM

Verwenden der AWS Security Incident Response-Konsole

Um darauf zugreifen zu können <https://console.aws.amazon.com/security-ir/>, müssen Sie über ein Mindestmaß an Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, die Ressourcen zur Reaktion auf AWS Sicherheitsvorfälle in Ihrem AWS Konto aufzulisten und einzusehen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur Anrufe an AWS CLI oder am tätigen, keine Mindestberechtigungen für die Konsole gewähren AWS API. Erlauben Sie stattdessen nur den Zugriff auf die Aktionen, die dem API Vorgang entsprechen, den sie ausführen möchten.

Fügen Sie den AWS Security Incident Response Access oder die ReadOnly AWS verwaltete Richtlinie hinzu, um sicherzustellen, dass Benutzer und Rollen die Servicekonsole verwenden können. Weitere Informationen finden Sie im [Benutzerhandbuch unter Hinzufügen von Berechtigungen für einen IAM](#) Benutzer.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der Inline-Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von oder. AWS CLI AWS API

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
```

```
"iam:GetUserPolicy",
"iam:ListGroupsWithUser",
"iam:ListAttachedUserPolicies",
"iam:ListUserPolicies",
"iam:GetUser"
],
"Resource": ["arn:aws:iam::*:user/${AWS:username}"]
},
{
  "Sid": "NavigateInConsole",
  "Effect": "Allow",
  "Action": [
    "iam:GetGroupPolicy",
    "iam:GetPolicyVersion",
    "iam:GetPolicy",
    "iam:ListAttachedGroupPolicies",
    "iam:ListGroupPolicies",
    "iam:ListPolicyVersions",
    "iam:ListPolicies",
    "iam:ListUsers"
  ],
  "Resource": "*"
}
]
```

Ressourcenbasierte Richtlinien innerhalb von Security Incident Response AWS

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS -Services umfassen.

Weitere Informationen finden Sie unter [Kontenübergreifender Ressourcenzugriff IAM im IAM Benutzerhandbuch](#).

Politische Maßnahmen zur Reaktion auf AWS Sicherheitsvorfälle

Politische Maßnahmen Support: Ja

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

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

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der Aktionen zur Reaktion auf AWS Sicherheitsvorfälle finden Sie in der Serviceautorisierungsreferenz unter Aktionen, die durch die Reaktion auf AWS Sicherheitsvorfälle definiert wurden.

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

AWS Reaktion auf Sicherheitsvorfälle — Identität

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

„Aktion“: [„Reaktion auf AWS Sicherheitsvorfälle -identity:action1“, „Reaktion auf Sicherheitsvorfälle -identity:action2“]AWS

Richtlinienressourcen für Amazon AWS Security Incident Response

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

Das JSON Ressourcenrichtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder eine Ressource oder ein NotResource Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem [Amazon-Ressourcennamen \(ARN\)](#) anzugeben. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

"Resource": "*"

Schlüssel zu den Richtlinienbedingungen für die Reaktion auf AWS Sicherheitsvorfälle

Unterstützt dienstspezifische Richtlinien-Bedingungsschlüssel: Nein

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

Mit dem Condition-Element (oder dem Bedingungsblock) können Sie Bedingungen angeben, unter denen eine Aussage gültig ist. Das Bedingungs-element ist optional. Sie können bedingte Ausdrücke erstellen, die [Bedingungsoperatoren](#) verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere Condition-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzigen Condition-Element angeben, werden diese mithilfe einer logischen AND Operation AWS ausgewertet. Wenn Sie mehrere Werte für einen einzelnen Bedingungs-schlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen OR-Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [IAMRichtlinienelemente: Variablen und Tags](#).

AWS unterstützt globale Bedingungs-schlüssel und dienstspezifische Bedingungs-schlüssel. Eine Übersicht aller AWS globalen Bedingungs-schlüssel finden Sie unter [Kontext-Schlüssel für AWS globale Bedingungen](#) im IAMBenutzerhandbuch.

Zugriffskontrolllisten (ACLs) in AWS Security Incident Response

UnterstütztACLs: Nein

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

Attributbasierte Zugriffskontrolle () ABAC mit Reaktion auf Sicherheitsvorfälle AWS

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC Richtlinien, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt, auf die er zugreifen möchte. ABAC ist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie Tag-Informationen im [Condition-Element einer Richtlinie mit den Bedingungsschlüsseln](#) AWS: ResourceTag /key-name, /key-name AWS oder: RequestTag ein. AWS TagKeys Wenn ein Dienst alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, ist der Wert für den Dienst Ja. Wenn ein Dienst alle drei Bedingungsschlüssel nur für einige Ressourcentypen unterstützt, ist der Wert Partial. Weitere Informationen zu ABAC finden Sie unter [Was ist ABAC?](#) im IAM Benutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter [Verwenden der attributbasierten Zugriffskontrolle \(ABAC\)](#). IAM

Temporäre Anmeldeinformationen mit Amazon AWS Security Incident Response

Unterstützt temporäre Anmeldeinformationen: Ja

AWS Dienste funktionieren nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich der AWS Dienste, die mit temporären Anmeldeinformationen funktionieren, finden Sie IAM im IAM Benutzerhandbuch unter [AWS Dienste, mit denen gearbeitet](#) werden kann. Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen Methode als einem Benutzernamen und einem Kennwort bei der AWS Management Console anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Rollenwechsel finden Sie unter [Wechseln zu einer Rolle \(Konsole\)](#) im IAM Benutzerhandbuch.

Mit dem AWS CLI oder können Sie manuell temporäre Anmeldeinformationen erstellen AWS API. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt

langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter [Temporäre Sicherheitsanmeldeinformationen unter IAM](#).

Zugriffssitzungen für AWS Security Incident Response weiterleiten

Unterstützt Forward-Access-Sitzungen (FAS): Ja

Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Wenn Sie einige Dienste verwenden, führen Sie möglicherweise eine Aktion aus, die dann eine weitere Aktion in einem anderen Dienst auslöst. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS Dienst aufruft, in Kombination mit dem anfordernden AWS Dienst, um Anfragen an nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS Diensten oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien beim Stellen von FAS Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

Behebung von AWS Sicherheitsvorfällen, Identität und Zugriff

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

Themen

- Ich bin nicht zur Ausführung einer Aktion autorisiert.
- Ich bin nicht berechtigt, iam durchzuführen: PassRole
- Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine Ressourcen zur Reaktion auf AWS Sicherheitsvorfälle ermöglichen

Ich bin nicht berechtigt, eine Aktion durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM Benutzer mateojackson versucht, die Konsole zu verwenden, um Details zu einer fiktiven my-example-widget Ressource anzuzeigen, aber nicht über die fiktiven Berechtigungen für AWS Security Incident Response: verfügt. GetWidget

Benutzer: arn ::iam: :123456789012:user/mateojackson ist nicht berechtigt, Folgendes auszuführen
AWS: Antwort auf Sicherheitsvorfälle: on resource: my -example-widget AWS GetWidget

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

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

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

Bei einigen AWS Diensten können Sie eine bestehende Rolle an diesen Dienst übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM Benutzer namens marymajor versucht, die Konsole zu verwenden, um eine Aktion in AWS Security Incident Response auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

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

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine Ressourcen zur Reaktion auf AWS Sicherheitsvorfälle ermöglichen

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

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Amazon AWS Security Incident Response diese Funktionen unterstützt, finden Sie unter [So funktioniert AWS Security Incident Response mitIAM](#).
- Informationen dazu, wie Sie den Zugriff auf Ihre Ressourcen mit Ihren AWS Konten gewähren können, finden Sie im Benutzerhandbuch unter [Gewähren des Zugriffs auf einen IAM Benutzer in einem anderen AWS Konto, das IAM Sie besitzen](#).

- Informationen dazu, wie Sie AWS Konten von Drittanbietern Zugriff auf Ihre Ressourcen [gewähren können, finden Sie im IAMBenutzerhandbuch unter Gewähren des Zugriffs auf AWS Konten Dritter](#).
- Informationen dazu, wie Sie Zugriff über einen Identitätsverbund [gewähren, finden Sie im Benutzerhandbuch unter Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#). IAM
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie [IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff](#). IAM

Verwenden von Servicerollen

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine [IAMRolle](#), die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [Erstellen einer Rolle zum Delegieren von Berechtigungen für einen AWS Dienst](#).

Verwenden von serviceverknüpften Rollen

Dienstbezogene Rollen für die Reaktion auf AWS Sicherheitsvorfälle

Inhalt

- [AWS SLR: AWSServiceRoleForSecurityIncidentResponse](#)
- [AWS SLR: AWSServiceRoleForSecurityIncidentResponse_Triage](#)
- [Unterstützte Regionen für dienstbezogene Rollen im Zusammenhang mit AWS Security Incident Response](#)

Unterstützt dienstbezogene Rollen: Ja

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

Eine dienstbezogene Rolle erleichtert die Einrichtung von AWS Security Incident Response, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Security Incident Response definiert die Berechtigungen seiner dienstbezogenen Rollen, und sofern nicht anders

definiert, kann nur AWS Security Incident Response diese Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Informationen zu anderen Diensten, die dienstbezogene Rollen unterstützen, finden Sie unter [AWS Dienste, die mit Diensten funktionieren](#), IAM und suchen Sie in der Spalte Dienstbezogene Rollen nach Diensten, für die Ja steht. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

AWS SLR: AWSServiceRoleForSecurityIncidentResponse

AWS Security Incident Response verwendet die mit dem Dienst verknüpfte Rolle (SLR) mit dem AWSServiceRoleForSecurityIncidentResponse Namen AWS Security Incident Response-Richtlinie, um abonnierte Konten zu identifizieren, Fälle zu erstellen und zugehörige Ressourcen zu kennzeichnen.

Berechtigungen

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

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

Dieser Rolle ist die AWS verwaltete Richtlinie mit dem Namen zugeordnet.

[AWSSecurityIncidentResponseServiceRolePolicy](#) Der Dienst verwendet die Rolle, um Aktionen für die folgenden Ressourcen durchzuführen:

- AWS Organizations: Ermöglicht dem Dienst, nach Mitgliedskonten für die Verwendung mit dem Dienst zu suchen.
- CreateCase: Ermöglicht dem Dienst, Servicefälle im Namen von Mitgliedskonten zu erstellen.
- TagResource: Ermöglicht die Service-Tag-Ressourcen, die als Teil des Dienstes konfiguriert wurden.

Die Rolle verwalten

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie zu AWS Security Incident Response im AWS Management Console, dem oder dem wechseln AWS CLI AWS API, erstellt der Service die dienstbezogene Rolle für Sie.

Note

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

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

Sie müssen Berechtigungen konfigurieren, damit eine IAM-Entität (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen können. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [Berechtigungen für dienstbezogene Rollen](#).

AWS SLR: AWSServiceRoleForSecurityIncidentResponse_Triage

AWS Security Incident Response verwendet die servicebezogene Rolle (SLR) mit dem Namen AWSServiceRoleForSecurityIncidentResponse_Triage AWS Security Incident Response-Richtlinie, um Ihre Umgebung kontinuierlich auf Sicherheitsbedrohungen zu überwachen, Sicherheitsdienste zu optimieren, um Warngeräusche zu reduzieren, und Informationen zur Untersuchung potenzieller Vorfälle zu sammeln.

Berechtigungen

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

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

Dieser Rolle ist die AWS verwaltete Richtlinie zugeordnet.

[AWSSecurityIncidentResponseTriageServiceRolePolicy](#) Der Dienst verwendet die Rolle, um Aktionen für die folgenden Ressourcen durchzuführen:

- Ereignisse: Ermöglicht dem Dienst, eine Amazon EventBridge verwaltete Regel zu erstellen. Diese Regel ist die Infrastruktur, die in Ihrem AWS Konto erforderlich ist, um Ereignisse von Ihrem Konto an den Dienst zu übertragen. Diese Aktion wird für jede AWS Ressource ausgeführt, die von verwaltet wird `triage.security-ir.amazonaws.com`.

- Amazon GuardDuty: Ermöglicht dem Service, die Sicherheitsdienste zu optimieren, um Warngeräusche zu reduzieren und Informationen zur Untersuchung potenzieller Vorfälle zu sammeln. Diese Aktion wird für jede AWS Ressource ausgeführt.
- AWS Security Hub: Ermöglicht dem Dienst, Sicherheitsdienste zu optimieren, um Warngeräusche zu reduzieren und Informationen zur Untersuchung potenzieller Vorfälle zu sammeln. Diese Aktion wird für jede AWS Ressource ausgeführt.

Die Rolle verwalten

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie zu AWS Security Incident Response im AWS Management Console, dem oder dem wechseln AWS CLI AWS API, erstellt der Service die dienstbezogene Rolle für Sie.

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

Sie müssen Berechtigungen konfigurieren, damit eine IAM-Entität (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen können. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [Berechtigungen für dienstbezogene Rollen](#).

Unterstützte Regionen für dienstbezogene Rollen im Zusammenhang mit AWS Security Incident Response

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

- USA Ost (Ohio)
- USA West (Oregon)
- USA Ost (Virginia)
- EU (Frankfurt)
- EU (Irland)
- EU (London)
- EU (Stockholm)
- Asien-Pazifik (Singapur)
- Asia Pacific (Seoul)

- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Canada (Central)

AWS Verwaltete Richtlinien

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet AWS wird. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von [IAM-Kunden verwaltete Richtlinien zu erstellen](#), die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAMBenutzerhandbuch unter [AWS Verwaltete Richtlinien](#).

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

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und eine Beschreibung der Richtlinien für Jobfunktionen finden Sie im IAMBenutzerhandbuch unter [AWS Verwaltete Richtlinien für Jobfunktionen](#).

Inhalt

- [AWS verwaltete Richtlinie: AWSSecurityIncidentResponseServiceRolePolicy](#)

- [AWS verwaltete Richtlinie: AWSSecurityIncidentResponseFullAccess](#)
- [AWS verwaltete Richtlinie: AWSSecurityIncidentResponseReadOnlyAccess](#)
- [AWS verwaltete Richtlinie: AWSSecurityIncidentResponseCaseFullAccess](#)
- [AWS verwaltete Richtlinie: AWSSecurityIncidentResponseTriageServiceRolePolicy](#)
- [AWS Security Incident Response aktualisiert SLRs und verwaltet Richtlinien](#)

AWS verwaltete Richtlinie:

AWSSecurityIncidentResponseServiceRolePolicy

AWS Security Incident Response verwendet die AWSSecurityIncidentResponseServiceRolePolicy AWS verwaltete Richtlinie. Diese AWS verwaltete Richtlinie ist der [AWSServiceRoleForSecurityIncidentResponse](#) dienstbezogenen Rolle zugeordnet. Die Richtlinie bietet Zugriff auf AWS Security Incident Response, um abonnierte Konten zu identifizieren, Fälle zu erstellen und zugehörige Ressourcen zu taggen.

Important

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

Einzelheiten zu den Berechtigungen

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

- **AWS Organizations:** Ermöglicht dem Dienst, nach Mitgliedskonten für die Verwendung mit dem Dienst zu suchen.
- **CreateCase:** Ermöglicht dem Dienst, Servicefälle im Namen von Mitgliedskonten zu erstellen.
- **TagResource:** Ermöglicht die Service-Tag-Ressourcen, die als Teil des Dienstes konfiguriert wurden.

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

AWS verwaltete Richtlinie: AWSSecurityIncidentResponseFullAccess

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

Important

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

Einzelheiten zu den Berechtigungen

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

- IAMNur-Lese-Zugriff für den Prinzipal: Gewährt einem Servicebenutzer die Möglichkeit, schreibgeschützte Aktionen für vorhandene Ressourcen zur Reaktion auf AWS Sicherheitsvorfälle durchzuführen.
- IAMPrinzipal-Schreibzugriff: Gewährt einem Servicebenutzer die Möglichkeit, Ressourcen zur Reaktion auf AWS Sicherheitsvorfälle zu aktualisieren, zu ändern, zu löschen und zu erstellen.

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

AWS verwaltete Richtlinie: AWSSecurityIncidentResponseReadOnlyAccess

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

⚠ Important

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

Einzelheiten zu den Berechtigungen

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

- IAMNur-Lese-Zugriff für den Prinzipal: Gewährt einem Servicebenutzer die Möglichkeit, schreibgeschützte Aktionen für vorhandene Ressourcen zur Reaktion auf AWS Sicherheitsvorfälle durchzuführen.

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

AWS verwaltete Richtlinie: AWSSecurityIncidentResponseCaseFullAccess

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

⚠ Important

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

Einzelheiten zu den Berechtigungen

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

- IAMNur-Lese-Zugriff im Prinzipfall: Gewährt einem Servicebenutzer die Möglichkeit, bei bestehenden AWS Security Incident Response-Fällen schreibgeschützte Aktionen durchzuführen.
- IAMSchreibzugriff für Principal Case: Gewährt einem Servicebenutzer die Möglichkeit, AWS Security Incident Response-Fälle zu aktualisieren, zu ändern, zu löschen und zu erstellen.

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

AWS verwaltete Richtlinie:

AWSSecurityIncidentResponseTriageServiceRolePolicy

AWS Security Incident Response verwendet die AWSSecurityIncidentResponseTriageServiceRolePolicy AWS verwaltete Richtlinie. Diese AWS verwaltete Richtlinie ist der mit dem Dienst verknüpften [AWSServiceRoleForSecurityIncidentResponseRolle _Triage](#) zugeordnet.

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

Important

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

Einzelheiten zu den Berechtigungen

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

- Ereignisse: Ermöglicht dem Service, eine von Amazon EventBridge verwaltete Regel zu erstellen. Diese Regel ist die Infrastruktur, die in Ihrem AWS Konto erforderlich ist, um Ereignisse von Ihrem Konto an den Service zu übertragen. Diese Aktion wird für jede AWS Ressource ausgeführt, die von verwaltet wird `triage.security-ir.amazonaws.com`.

- Amazon GuardDuty: Ermöglicht dem Service, die Sicherheitsdienste zu optimieren, um Warngeräusche zu reduzieren und Informationen zur Untersuchung potenzieller Vorfälle zu sammeln. Diese Aktion wird für jede AWS Ressource ausgeführt.
- AWS Security Hub: Ermöglicht dem Dienst, Sicherheitsdienste zu optimieren, um Warngeräusche zu reduzieren und Informationen zur Untersuchung potenzieller Vorfälle zu sammeln. Diese Aktion wird für jede AWS Ressource ausgeführt.

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

AWS Security Incident Response aktualisiert SLRs und verwaltet Richtlinien

Hier finden Sie Informationen zu Aktualisierungen der Rollen „AWS Security Incident Response“ SLRs und „verwaltete Richtlinien“, die seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden.

Änderung	Beschreibung	Datum
Neu SLR — AWSServiceRoleForSecurityIncidentResponse	Neue dienstbezogene Rolle und angehängte Richtlinie, die den Dienstzugriff auf Ihre AWS Organizations Konten ermöglichen, um die Mitgliedschaft zu identifizieren.	01. Dezember 2024
Neue verwaltete Richtlinie — AWSSecurityIncidentResponseServiceRolePolicy		
Neu SLR — AWSServiceRoleForSecurityIncidentResponse_Triage	Neue dienstbezogene Rolle und angehängte Richtlinie, die den Dienstzugriff auf Ihre AWS Organizations Konten ermöglicht, um Sicherheitsereignisse zu sortieren.	01. Dezember 2024

Änderung	Beschreibung	Datum
Neue verwaltete Richtlinie — AWSSecurityIncidentResponseTriageServiceRolePolicy		
Neue verwaltete Richtlinie — AWSSecurityIncidentResponseFullAccess	AWS Security Incident Response fügt eine neue SLR hinzu, die den IAM Prinzipalen für Lese- und Schreibaktionen für den Service angehängt werden kann.	01. Dezember 2024
Neue Rolle für verwaltete Richtlinien — AWSSecurityIncidentResponseReadOnlyAccess	AWS Security Incident Response fügt eine neue hinzuSLR, die an IAM Principals für Leseaktionen angehängt werden kann	01. Dezember 2024
Neue Rolle für verwaltete Richtlinien — AWSSecurityIncidentResponseCaseFullAccess	AWS Security Incident Response fügt eine neue Funktion SLR hinzu, die den IAM Hauptbenutzern für Lese- und Schreibaktionen für Servicefälle angehängt werden kann.	01. Dezember 2024
Die Nachverfolgung von Änderungen wurde gestartet.	Die Nachverfolgung von Änderungen in Bezug auf AWS Security Incident Response SLRs und verwaltete Richtlinien wurde gestartet	01. Dezember 2024

Vorfallreaktion

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

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

Compliance-Validierung

Externe Prüfer bewerten die Sicherheit und Konformität von AWS Services im Rahmen mehrerer AWS Compliance-Programme. Dazu gehören SOC PCI RAMPHIPAA, Fed und andere.

AWS Die Reaktion auf Sicherheitsvorfälle wurde nicht im Hinblick auf die Einhaltung der oben genannten Programme bewertet.

Eine Liste der AWS Services im Rahmen bestimmter Compliance-Programme finden Sie unter [AWS Services im Umfang der einzelnen Compliance-Programme](#). Allgemeine Informationen finden Sie unter [AWS Compliance-Programme](#).

Mit AWS Artifact können Sie Prüfberichte von Drittanbietern herunterladen. Weitere Informationen finden Sie unter [Berichte in AWS Artifact herunterladen](#).

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung von AWS Diensten hängt von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Vorschriften AWS ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- [Schnellstartanleitungen zu Sicherheit und Compliance](#) — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Umgebungen

beschrieben, auf denen auf Sicherheit und Compliance ausgerichtete Basisumgebungen eingerichtet werden. AWS

- Whitepaper [Architecting for HIPAA Security and Compliance — In diesem Whitepaper](#) wird beschrieben, wie Unternehmen damit -konforme Anwendungen erstellen können AWS . HIPAA
- [AWS Compliance-Ressourcen](#) — Eine Sammlung von Arbeitsmappen und Leitfäden, die je nach Branche und/oder Standort relevant sind.
- [Evaluierung von Ressourcen mit AWS Config Rules](#) im AWS Config Developer Guide — AWS Config; bewertet, wie gut Ihre Ressourcenkonfigurationen internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- [AWS Security Hub](#) — Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb AWS. Security Hub verwendet Sicherheitskontrollen, um Ihre AWS Ressourcen zu bewerten und Ihre Einhaltung der Sicherheitsstandards und Best Practices der Sicherheitsbranche zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der [Security-Hub-Steuerungsreferenz](#).
- [Amazon GuardDuty](#) — Dieser AWS Service erkennt potenzielle Bedrohungen für Ihre AWS Konten, Workloads, Container und Daten, indem er Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen zu erfüllen PCIDSS, z. B. durch die Erfüllung der Anforderungen zur Erkennung von Eindringlingen, die in bestimmten Compliance-Frameworks vorgeschrieben sind.
- [AWS Audit Manager](#) — Mit diesem AWS Service können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um Ihr Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Protokollierung und Überwachung in AWS Security Incident Response

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

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

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

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

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

Ausfallsicherheit

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter [AWS Globale Infrastruktur](#).

Sicherheit der Infrastruktur

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

Sie verwenden AWS veröffentlichte API Aufrufe, um über das Netzwerk auf AWS Security Incident Response zuzugreifen. Kunden müssen Folgendes unterstützen:

- Sicherheit auf Transportschicht (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Cipher-Suites mit perfekter Vorwärtsgeheimhaltung (PFS) wie (Ephemeral Diffie-Hellman) oder DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

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

Konfigurations- und Schwachstellenanalyse

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

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

- [Modell der geteilten Verantwortung](#)
- [Bewährte Methoden für Sicherheit, Identität und Compliance](#)

Serviceübergreifende Confused-Deputy-Prävention

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

Wir empfehlen die Verwendung der SourceAccount globalen Bedingungskontextschlüssel [AWS:SourceArn](#) [und](#): in Ressourcenrichtlinien, um die Berechtigungen einzuschränken, die Amazon

Connect einem anderen Service für die Ressource erteilt. Wenn Sie beide Kontextschlüssel für globale Bedingungen verwenden, müssen der SourceAccount Wert AWS: und das Konto im SourceArn Wert AWS: dieselbe Konto-ID verwenden, wenn sie in derselben Richtlinienerklärung verwendet werden.

Der effektivste Weg, sich vor dem Problem des verwirrten Stellvertreters zu schützen, besteht darin, den exakten Amazon-Ressourcennamen (ARN) der Ressource zu verwenden, die Sie zulassen möchten. Wenn Sie die Ressource nicht vollständig ARN kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den Bedingungsschlüssel AWS: SourceArn globaler Kontext mit Platzhaltern (*) für die unbekanntenen Teile von. ARN Zum Beispiel arn ::servicename: :region-name AWS: :your account ID: *. AWS

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

Service Quotas

AWS Reaktion auf Sicherheitsvorfälle

In den folgenden Tabellen sind die Kontingente für Ressourcen zur Reaktion auf AWS Sicherheitsvorfälle für Ihr AWS Konto aufgeführt;. Einige Kontingente können mit Zustimmung des Service Managers über die unten angegebenen Werte hinaus erhöht werden. Sofern nicht anders angegeben, gelten diese Kontingente pro Region.

	Name	Standard	Anpassbar	Kommentare
1	Aktive AWS unterstützte Fälle	10	Ja (bis zu 50)	Die Anzahl der aktiven Fälle, bei denen Unterstützung angefordert wurde AWS CIRT.
2	Aktive, selbst verwaltete Fälle	50	Ja (bis zu 100)	Die Anzahl der aktiven Fälle, die die Plattform ohne Unterstützung von nutzen AWS CIRT.
3	Vom Service unterstützte Fälle, die innerhalb von 24 Stunden erstellt wurden	10	Nein	Die Anzahl der innerhalb eines 24-stündigen Zeitfensters AWS CIRT erstellten Fälle, in denen um Unterstützung gebeten wurde.
4	Maximale Anzahl von Entitäten	10	Nein	Die maximale Anzahl von

	Name	Standard	Anpassbar	Kommentare
	im Standard-Incident-Response-Team			Entitäten im Standard-Incident-Response-Team.
5	Maximale Anzahl zusätzlicher Mitglieder für einen Fall	30	Nein	Die maximale Anzahl von Entitäten, die mit einem Fall verknüpft sind. Dies wird zunächst mit Entitäten aus Ihrem Standard-Incident-Response-Team gefüllt.
6	Maximale Anzahl von Fallanhängen	50	Ja (bis zu 100)	Die maximale Anzahl von Dateien, die an einen Fall angehängt werden können.
7	Maximale Größe von Fallkommentaren	1000	Nein	Die maximale Anzahl von Zeichen in einem Fallkommentar.
8	Maximale Größe des Dateinamens von Fallanhängen	255	Nein	Die maximale Anzahl von Zeichen in einem Dateinamen.

AWS Technischer Leitfaden zur Reaktion auf Sicherheitsvorfälle

Inhalt

- [Überblick](#)
- [Sind Sie Well-Architected?](#)
- [Einführung](#)
- [Vorbereitung](#)
- [Operationen](#)
- [Aktivität nach Vorfällen](#)
- [Schlussfolgerung](#)
- [Mitwirkende](#)
- [Anhang A: Definitionen der Cloud-Funktionen](#)
- [Anhang B: Ressourcen zur Reaktion auf AWS Vorfälle](#)
- [Hinweise](#)

Überblick

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

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

Sind Sie Well-Architected?

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

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

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

Einführung

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

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

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

Bevor Sie beginnen

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

AWS Sicherheitsstandards und Frameworks

Zu Beginn empfehlen wir Ihnen, sich das Whitepaper [Best Practices for Security, Identity and Compliance, Security Pillar — AWS Well-Architected Framework](#) und The [Security Perspective of the Overview of the AWS Cloud Adoption Framework \(AWS CAF\)](#) durchzulesen.

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

Branchenübliche Standards und Rahmenbedingungen für die Reaktion auf Vorfälle

Dieses Whitepaper folgt den Standards und bewährten Verfahren zur Reaktion auf Vorfälle aus dem [Computer Security Incident Handling Guide SP 800-61 r2](#), der vom National Institute of Standards and Technology (NIST) erstellt wurde. Das Lesen und Verstehen der von eingeführten Konzepte NIST ist eine hilfreiche Voraussetzung. Die Konzepte und bewährten Verfahren aus diesem NIST Leitfaden werden in diesem paper auf AWS Technologien angewendet. Vorfallszenarien vor Ort fallen jedoch nicht in den Anwendungsbereich dieses Leitfadens.

AWS Überblick über die Reaktion auf Vorfälle

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

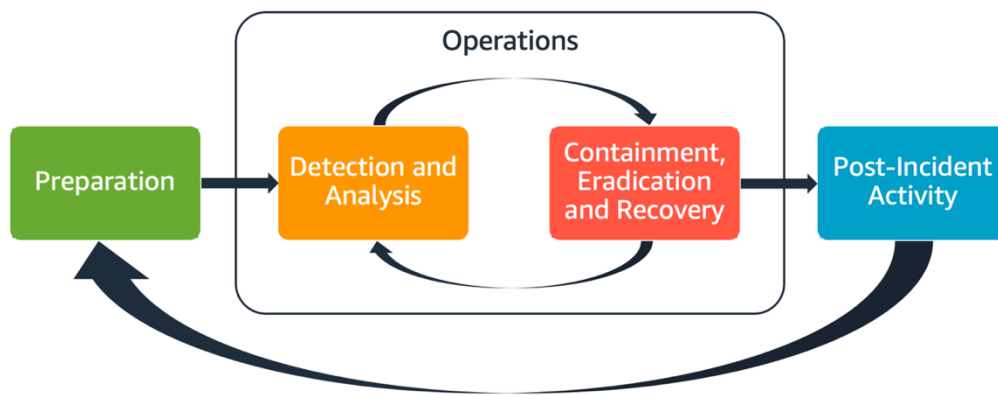
Aspekte der Reaktion auf AWS Vorfälle

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

Im Folgenden werden diese Aspekte genauer beschrieben:

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

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



Aspekte der Reaktion auf AWS Vorfälle

AWS Prinzipien und Entwurfsziele für die Reaktion auf Vorfälle

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

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

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

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

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

Domänen für Sicherheitsvorfälle in der Cloud

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

- Dienstdomäne — Vorfälle in der Dienstdomäne können sich auf Ihre AWS-Konto, [AWS Identity and Access Management](#)(IAM) -Berechtigungen, Ressourcenmetadaten, die Abrechnung oder andere Bereiche auswirken. Ein Dienstdomänenereignis ist ein Ereignis, auf das Sie ausschließlich mit AWS API Mechanismen reagieren oder bei dem Sie grundlegende Ursachen haben, die mit Ihrer

Konfiguration oder Ihren Ressourcenberechtigungen zusammenhängen, und möglicherweise mit einer zugehörigen serviceorientierten Protokollierung verbunden sind.

- **Infrastrukturdomäne** — Zu Vorfällen in der Infrastrukturdomäne gehören daten- oder netzwerkbezogene Aktivitäten, wie Prozesse und Daten auf Ihren [Amazon Elastic Compute Cloud](#) (AmazonEC2) -Instances, Datenverkehr zu Ihren EC2 Amazon-Instances innerhalb der Virtual Private Cloud (VPC) und andere Bereiche, wie Container oder andere future Dienste. Ihre Reaktion auf Ereignisse in der Infrastrukturdomäne beinhaltet häufig die Erfassung von vorfallbezogenen Daten für forensische Analysen. Dies beinhaltet wahrscheinlich die Interaktion mit dem Betriebssystem einer Instanz und kann in verschiedenen Fällen auch Mechanismen beinhalten. AWS API Im Infrastrukturbereich können Sie eine Kombination aus Tools für digitale Forensik/Incident Response (DFIR) innerhalb eines Gastbetriebssystems verwenden, z. B. eine EC2 Amazon-Instance, die für die Durchführung forensischer Analysen und Untersuchungen vorgesehen ist. AWS APIs Bei Infrastrukturdomänenvorfällen können Netzwerkpaketerfassungen, Festplattenblöcke auf einem [Amazon Elastic Block Store \(AmazonEBS\)](#) -Volume oder flüchtiger Speicher, der von einer Instance abgerufen wurde, analysiert werden.
- **Anwendungsdomäne** — Vorfälle in der Anwendungsdomäne treten im Anwendungscode oder in der Software auf, die für die Dienste oder die Infrastruktur bereitgestellt wird. Diese Domain sollte in Ihren Playbooks zur Erkennung und Abwehr von Cloud-Bedrohungen enthalten sein und könnte ähnliche Reaktionen wie die Infrastrukturdomäne beinhalten. Mit einer geeigneten und durchdachten Anwendungsarchitektur können Sie diese Domäne mithilfe von Cloud-Tools verwalten, indem Sie automatische Erfassung, Wiederherstellung und Bereitstellung nutzen.

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

Die wichtigsten Unterschiede bei der Reaktion auf Vorfälle sind AWS

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

beginnen, wenn Kunden beginnen, diese Muster in der Cloud zu entwerfen und zu entwickeln. Im Folgenden sind die wichtigsten Unterschiede bei der Reaktion auf Vorfälle in AWS aufgeführt.

Unterschied #1: Sicherheit als gemeinsame Verantwortung

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

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

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

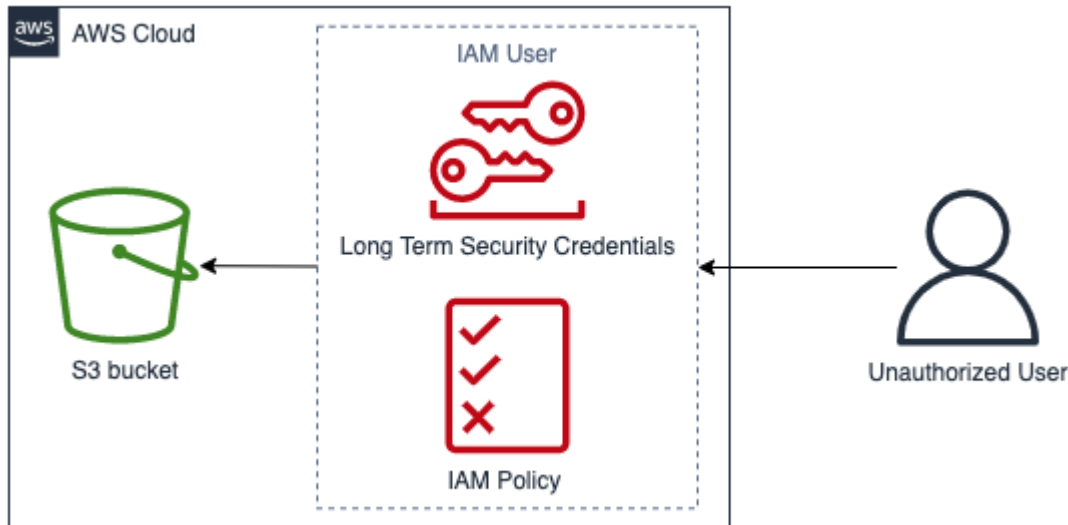
Es ist äußerst wichtig, einen geeigneten Plan zur Reaktion auf Vorfälle und entsprechende Playbooks zu erstellen und zu testen, die zu Ihrem Betriebsmodell passen.

Unterschied #2: Cloud-Dienstdomäne

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

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

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



Beispiel für eine Dienstdomäne

Unterschied #3: APIs für die Bereitstellung der Infrastruktur

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

Aufgrund des API basierten Charakters von AWS ist es eine wichtige Protokollquelle für die Reaktion auf Sicherheitsereignisse. Sie verfolgt die API Verwaltungsanrufe AWS CloudTrail, die in Ihren AWS Konten getätigt wurden, und in der Sie Informationen über den Quellort der API Anrufe finden können.

Unterschied #4: Dynamischer Charakter der Cloud

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

Unterschied #5: Datenzugriff

Der Datenzugriff ist auch in der Cloud anders. Sie können sich nicht an einen Server anschließen, um die Daten zu sammeln, die Sie für eine Sicherheitsuntersuchung benötigen. Die Daten werden über das Kabel und über API Anrufe gesammelt. Sie müssen lernen und verstehen, wie die Datenerfassung funktioniert, um auf diese Umstellung vorbereitet zu sein. APIs Außerdem müssen Sie sicherstellen, dass die Datenerfassung und der Zugriff auf die Daten angemessen sind.

Unterschied #6: Bedeutung der Automatisierung

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

Beseitigung dieser Unterschiede

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

Vorbereitung

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

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

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

Personen

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

Definieren von Rollen und Zuständigkeiten

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

Bei einem Vorfall ist es wichtig, die Eigentümer/Entwickler der betroffenen Anwendungen und Ressourcen einzubeziehen, da es sich um Fachexperten (SMEs) handelt, die Informationen

und den Kontext bereitstellen können, um die Auswirkungen zu messen. Üben Sie und bauen Sie Beziehungen zu den Entwicklern und Anwendungsbesitzern auf, bevor Sie sich bei der Vorfalldiagnose auf deren Fachwissen verlassen. Anwendungsbesitzer oder SMEs, wie z. B. Ihre Cloud-Administratoren oder Techniker, müssen möglicherweise in Situationen handeln, in denen die Umgebung unbekannt ist oder komplex ist oder in denen die Responder keinen Zugriff haben.

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

Schulen Sie Mitarbeiter für die Reaktion auf Vorfälle

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

AWS Cloud Technologien verstehen

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

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

Verstehen Sie Ihre AWS Umgebung

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

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

Machen Sie sich mit AWS Reaktionsteams und Support vertraut

Support

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

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

Wenn Sie einen Missbrauch melden müssen, wenden Sie sich außerdem an das [AWS Team für Vertrauen und Sicherheit](#).

AWS Team zur Reaktion auf Kundenvorfälle (CIRT)

Das AWS Customer Incident Response Team (CIRT) ist ein spezialisiertes, stets verfügbares globales AWS Team, das Kunden bei aktiven Sicherheitsvorfällen auf Kundenseite im Rahmen des [Modells der AWS gemeinsamen Verantwortung](#) unterstützt.

Wenn es Sie AWS CIRT unterstützt, erhalten Sie Unterstützung bei der Suche und Wiederherstellung für ein aktives Sicherheitsereignis am AWS. Mithilfe von AWS Serviceprotokollen unterstützen sie Sie bei der Ursachenanalyse und geben Ihnen Empfehlungen für die Wiederherstellung. Sie bieten auch Sicherheitsempfehlungen und bewährte Verfahren, mit denen Sie future Sicherheitsereignisse vermeiden können.

AWS Kunden können sie AWS CIRT über eine [AWS Support-Anfrage kontaktieren](#).

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

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

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

- Kunden mit Support Enterprise-Tarifen:
 1. Konto und Abrechnung
 2. Service: Konto
 3. Kategorie: Sicherheit
 4. Schweregrad: Kritische Frage zum Geschäftsrisiko

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

DDoSUnterstützung bei der Reaktion

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

AWS Managed Services (AMS)

[AWS Managed Services](#) (AMS) ermöglicht die kontinuierliche Verwaltung Ihrer AWS Infrastruktur, sodass Sie sich auf Ihre Anwendungen konzentrieren können. Durch die Implementierung von Best Practices zur Wartung Ihrer Infrastruktur tragen Sie AMS dazu bei, Ihren betrieblichen Aufwand und Ihr Risiko zu reduzieren. AMS automatisiert gängige Aktivitäten wie Änderungsanforderungen, Überwachung, Patch-Management, Sicherheit und Backup-Services und bietet Services über den gesamten Lebenszyklus für die Bereitstellung, den Betrieb und den Support Ihrer Infrastruktur.

AMS übernimmt die Verantwortung für die Implementierung einer Reihe von Sicherheitsfunktionen und reagiert täglich als Erste auf Warnmeldungen. Wenn eine Warnung ausgelöst wird, AMS folgt sie einem Standardsatz automatisierter und manueller Abläufe, um sicherzustellen, dass eine konsistente Reaktion gewährleistet ist. Diese Playbooks werden den AMS Kunden beim Onboarding zur Verfügung gestellt, sodass sie eine Reaktion entwickeln und mit ihnen abstimmen können. AMS

Prozess

Die Entwicklung gründlicher und klar definierter Prozesse zur Reaktion auf Vorfälle ist der Schlüssel zu einem erfolgreichen und skalierbaren Incident-Response-Programm. Wenn ein Sicherheitsereignis eintritt, helfen Ihnen klare Schritte und Workflows dabei, rechtzeitig zu reagieren. Möglicherweise verfügen Sie bereits über Prozesse zur Reaktion auf Vorfälle. Unabhängig von Ihrem aktuellen Status ist es wichtig, Ihre Prozesse zur Vorfalle Reaktion regelmäßig zu aktualisieren, zu wiederholen und zu testen.

Entwickeln und testen Sie einen Plan zur Reaktion auf Vorfälle

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

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

Es hat sich bewährt, die out-of-band Kommunikation als Backup für die Kommunikation bei Zwischenfällen zu nutzen. Ein Beispiel für eine Anwendung, die einen sicheren out-of-band Kommunikationskanal bereitstellt, ist [AWS Wickr](#).

- Phasen der Reaktion auf Vorfälle und zu ergreifende Maßnahmen — Führt die Phasen der Reaktion auf Vorfälle auf, z. B. Erkennung, Analyse, Beseitigung, Eindämmung und Wiederherstellung — einschließlich der in diesen Phasen zu ergreifenden Maßnahmen auf hoher Ebene
- Definitionen für Schweregrad und Priorisierung von Vorfällen — Erläutert, wie der Schweregrad eines Vorfalls klassifiziert wird, wie der Vorfall priorisiert wird und wie sich die Schweregraddefinitionen dann auf die Eskalationsverfahren auswirken

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

Dokumentieren und zentralisieren Sie Architekturdiagramme

Um schnell und präzise auf ein Sicherheitsereignis reagieren zu können, müssen Sie wissen, wie Ihre Systeme und Netzwerke aufgebaut sind. Das Verständnis dieser internen Muster ist nicht nur wichtig für die Reaktion auf Vorfälle, sondern auch für die Überprüfung der Konsistenz zwischen den Anwendungen, auf denen die Muster basieren, gemäß bewährten Methoden. Sie sollten auch sicherstellen, dass diese Dokumentation auf dem neuesten Stand ist und regelmäßig gemäß

neuen Architekturmustern aktualisiert wird. Sie sollten Dokumentationen und interne Repositorien entwickeln, in denen unter anderem folgende Elemente detailliert beschrieben werden:

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

- Werden Tickets automatisch erstellt?
- Welche Tools stehen zur Verfügung, um Protokolle für eine Untersuchung zu analysieren?
- Netzwerktopologie
 - Wie sind Geräte, Endpunkte und Verbindungen in Ihrem Netzwerk physisch oder logisch angeordnet?
 - Wie verbindet sich Ihr Netzwerk mit? AWS
 - Wie wird der Netzwerkverkehr zwischen Umgebungen gefiltert?
- Externe Infrastruktur
 - Wie werden nach außen gerichtete Anwendungen bereitgestellt?
 - Welche AWS Ressourcen sind öffentlich zugänglich?
 - Welche AWS Konten enthalten Infrastrukturen, die nach außen gerichtet sind?
 - Welche DDoS oder externe Filterung gibt es?

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

Entwickeln Sie Playbooks zur Reaktion auf Vorfälle

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

Wofür sollten Playbooks erstellt werden

Playbooks sollten für Vorfalldszenerarien wie die folgenden erstellt werden:

- Erwartete Vorfälle — Playbooks sollten für Vorfälle erstellt werden, die Sie erwarten. Dazu gehören Bedrohungen wie Denial of Service (DoS), Ransomware und die Kompromittierung von Anmeldeinformationen.
- Bekannte Sicherheitsfeststellungen oder Sicherheitswarnungen — Playbooks sollten für Ihre bekannten Sicherheitsfeststellungen und -warnungen, wie z. B. Ergebnisse, erstellt werden. GuardDuty Möglicherweise erhalten Sie ein GuardDuty Ergebnis und denken: „Was nun?“ Um

zu verhindern, dass ein GuardDuty Ergebnis falsch behandelt oder das Ergebnis ignoriert wird, sollten Sie für jedes potenzielle Ergebnis ein Playbook erstellen. GuardDuty [Einige Einzelheiten und Anleitungen zur Problembeseitigung finden Sie in der Dokumentation. GuardDuty](#) Es ist erwähnenswert, dass dies standardmäßig nicht aktiviert GuardDuty ist und Kosten verursacht. Weitere Einzelheiten dazu GuardDuty finden Sie in Anhang A: Definitionen der Cloud-Funktionen [-the section called "Sichtbarkeit und Alarmierung"](#).

Was sollte in Playbooks enthalten sein

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

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

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

Um die Konsistenz der Informationen in jedem Playbook zu überprüfen, kann es hilfreich sein, eine Playbook-Vorlage zu erstellen, die Sie in Ihren anderen Sicherheits-Playbooks verwenden können. Einige der zuvor aufgeführten Elemente, wie z. B. Informationen zu Interessengruppen, können von mehreren Playbooks gemeinsam genutzt werden. Wenn das der Fall ist, können Sie

eine zentrale Dokumentation für diese Informationen erstellen, im Playbook darauf verweisen und dann die expliziten Unterschiede im Playbook auflisten. Auf diese Weise müssen Sie nicht dieselben Informationen in all Ihren einzelnen Playbooks aktualisieren. Indem Sie eine Vorlage erstellen und allgemeine oder gemeinsam genutzte Informationen in Playbooks identifizieren, können Sie die Entwicklung von Playbooks vereinfachen und beschleunigen. Schließlich werden sich Ihre Playbooks wahrscheinlich im Laufe der Zeit weiterentwickeln. Sobald Sie sich vergewissert haben, dass die Schritte konsistent sind, bilden sich daraus die Voraussetzungen für die Automatisierung.

Beispiele für Playbooks

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

Führen Sie regelmäßige Simulationen durch

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


Simulationen bieten eine Vielzahl von Vorteilen, darunter:

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

Arten von Simulationen

Es gibt drei Hauptarten von Simulationen:

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

 Note

AWS verlangt von Kunden, dass sie die auf der [Penetrationstest-Website verfügbaren Richtlinien für Penetrationstests](#) lesen, bevor sie Purple Team- oder Red Team-Übungen durchführen.

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

Tabelle 1 — Arten von Simulationen

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

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

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

Lebenszyklus des Trainings

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

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

Technologie

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

Entwickeln AWS Sie die Kontostruktur

[AWS Organizations](#) hilft Ihnen dabei, eine AWS Umgebung zentral zu verwalten und zu steuern, während Sie Ihre AWS Ressourcen erweitern und skalieren. Eine AWS Organisation konsolidiert Ihre

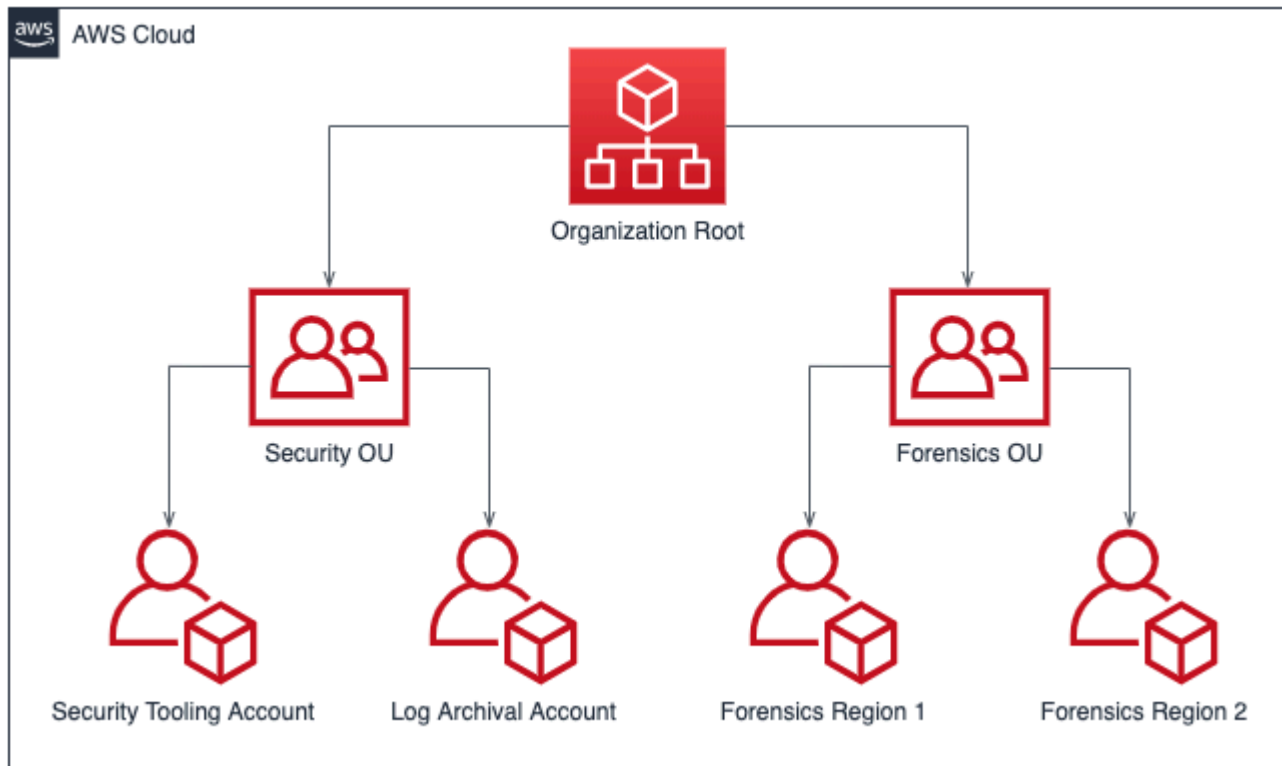
AWS Konten, sodass Sie sie als eine Einheit verwalten können. Sie können Organisationseinheiten (OUs) verwenden, um Konten zu gruppieren und sie als eine einzige Einheit zu verwalten.

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

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

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

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



Kontostruktur pro Region für die Reaktion auf Vorfälle

Entwickeln und Implementieren einer Markierungsstrategie

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

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

Kontaktinformationen für AWS das Konto aktualisieren

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

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

Für Kunden, die dies nutzen AWS Organizations, können Unternehmensadministratoren alternative Kontakte für Mitgliedskonten mithilfe des Verwaltungskontos oder eines delegierten Administratorkontos zentral verwalten, ohne dass für jedes Konto Anmeldeinformationen erforderlich sind. AWS Sie müssen außerdem überprüfen, ob neu erstellte Konten über korrekte Kontaktinformationen verfügen. Informationen zum [neu erstellten AWS-Konten Blogbeitrag finden Sie unter Alternative Kontakte automatisch aktualisieren](#).

Bereiten Sie den Zugriff auf vor AWS-Konten

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

Um diesen Zugriff zu implementieren und bereitzustellen, sollten Sie die AWS Kontostrategie und die Cloud-Identitätsstrategie mit den Cloud-Architekten Ihres Unternehmens besprechen und besprechen, um zu verstehen, welche Authentifizierungs- und Autorisierungsmethoden konfiguriert sind. Aufgrund des privilegierten Charakters dieser Anmeldeinformationen sollten Sie im Rahmen Ihrer Implementierung die Verwendung von Genehmigungsabläufen oder das Abrufen von

Anmeldeinformationen aus einem Tresor oder Safe in Betracht ziehen. Nach der Implementierung sollten Sie den Zugriff der Teammitglieder dokumentieren und testen, lange bevor ein Ereignis eintritt, um sicherzustellen, dass sie ohne Verzögerungen reagieren können.

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

Verstehen Sie die Bedrohungslandschaft

Entwickeln Sie Bedrohungsmodelle

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

Integrieren und nutzen Sie Informationen zu Cyberbedrohungen

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

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

Auswählen und Einrichten von Protokollen für die Analyse und Alarmierung

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

Wählen und aktivieren Sie Protokollquellen

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

AWS CloudTrail ist ein Protokollierungsdienst, der API Anrufe anhand der Aktivitäten eines AWS AWS Kontoerfassungsdienstes verfolgt. Er ist standardmäßig aktiviert und ermöglicht die 90-tägige Aufbewahrung von Verwaltungsereignissen, die [über CloudTrail die Funktion „Ereignisverlauf“ mit AWS Management Console AWS CLI, oder einem AWS SDK abgerufen](#) werden können. Für eine längere Aufbewahrung und Sichtbarkeit von Datenereignissen müssen Sie [einen CloudTrail Trail erstellen](#) und ihn einem Amazon S3 S3-Bucket und optional einer CloudWatch Protokollgruppe zuordnen. Alternativ können Sie einen [CloudTrail Lake](#) erstellen, der CloudTrail Protokolle bis zu sieben Jahre lang aufbewahrt und eine SQL basierte Abfragefunktion bietet.

AWS empfiehlt Kunden, Netzwerkdatenverkehr und DNS Logs mit [VPCFlow Logs bzw. Amazon Route 53 Resolver-Abfrageprotokollen](#) zu VPC aktivieren und diese entweder in einen Amazon S3 S3-Bucket oder eine CloudWatch Protokollgruppe zu streamen. Sie können ein VPC Flow-Protokoll für eine VPC, ein Subnetz oder eine Netzwerkschnittstelle erstellen. Bei VPC Flow Logs können Sie auswählen, wie und wo Sie Flow Logs aktivieren, um die Kosten zu senken.

AWS CloudTrail Logs, VPC Flow Logs und Route 53-Resolver-Abfrageprotokolle sind die grundlegenden Protokollierungs-Trifecta zur Unterstützung von Sicherheitsuntersuchungen. AWS

AWS Services können Protokolle generieren, die nicht von den grundlegenden Logging-Trifecta erfasst werden, wie z. B. Elastic Load Balancing AWS WAF Balancing-Logs, Logs, AWS Config Recorder-Logs, GuardDuty Amazon-Ergebnisse, Amazon Elastic Kubernetes Service (AmazonEKS) Audit-Logs und EC2 Amazon-Instance-Betriebssystem- und Anwendungsprotokolle. Die vollständige Liste der [the section called “Anhang A: Definitionen der Cloud-Funktionen”](#) Protokollierungs- und Überwachungsoptionen finden Sie unter.

Wählen Sie Protokollspeicher

Die Wahl des Protokollspeichers hängt im Allgemeinen vom verwendeten Abfragetool, den Aufbewahrungsmöglichkeiten, der Vertrautheit und den Kosten ab. Wenn Sie AWS Serviceprotokolle aktivieren, stellen Sie eine Speichereinrichtung bereit, normalerweise einen Amazon S3 S3-Bucket oder eine CloudWatch Protokollgruppe.

Ein Amazon S3 S3-Bucket bietet kostengünstigen, dauerhaften Speicher mit einer optionalen Lebenszyklusrichtlinie. In Amazon S3 S3-Buckets gespeicherte Protokolle können mithilfe von Diensten wie Amazon Athena nativ abgefragt werden. Eine CloudWatch Protokollgruppe bietet dauerhaften Speicherplatz und eine integrierte Abfragefunktion über Logs Insights. CloudWatch

Identifizieren Sie die geeignete Aufbewahrung von Protokollen

Wenn Sie einen S3-Bucket oder eine CloudWatch S3-Protokollgruppe zum Speichern von Protokollen verwenden, müssen Sie für jede Protokollquelle angemessene Lebenszyklen einrichten, um die Speicher- und Abrufkosten zu optimieren. Kunden stehen in der Regel zwischen 3 und 12 Monaten an Protokollen für Abfragen zur Verfügung, die bis zu sieben Jahre aufbewahrt werden können. Die Wahl von Verfügbarkeit und Aufbewahrungszeit sollte sich nach Ihren Sicherheitsanforderungen und einer Kombination aus gesetzlichen, regulatorischen und unternehmensinternen Vorschriften richten.

Wählen und implementieren Sie Abfragemechanismen für Protokolle

Die wichtigsten Dienste AWS, mit denen Sie Protokolle abfragen können, sind [CloudWatch Logs Insights](#) für in CloudWatch Protokollgruppen gespeicherte Daten sowie [Amazon Athena](#) und [Amazon OpenSearch Service](#) für in Amazon S3 gespeicherte Daten. Sie können auch Abfragetools von Drittanbietern verwenden, z. B. die Verwaltung von Sicherheitsinformationen und Ereignissen (SIEM).

Bei der Auswahl eines Tools zur Protokollabfrage sollten Sie die Personen, die Prozesse und die Technologieaspekte Ihrer Sicherheitsoperationen berücksichtigen. Wählen Sie ein Tool, das betriebliche, geschäftliche und Sicherheitsanforderungen erfüllt und sowohl zugänglich als auch langfristig wartbar ist. Denken Sie daran, dass Tools zur Protokollabfrage optimal funktionieren, wenn die Anzahl der zu durchsuchenden Protokolle im Rahmen der Limits des jeweiligen Tools liegt. Es ist nicht ungewöhnlich, dass Kunden aus Kosten- oder technischen Gründen über mehrere Abfragetools verfügen. Beispielsweise könnten Kunden einen Drittanbieter verwenden, SIEM um Abfragen für die Daten der letzten 90 Tage durchzuführen, und Athena für Abfragen verwenden, die länger als 90 Tage andauern, da die Protokollaufnahme von a kostet. SIEM Stellen Sie unabhängig von der Implementierung sicher, dass Ihr Ansatz die Anzahl der Tools minimiert, die zur Maximierung der betrieblichen Effizienz erforderlich sind, insbesondere bei der Untersuchung eines Sicherheitsvorfalls.

Verwenden Sie Protokolle für Warnmeldungen

AWS bietet nativ Benachrichtigungen über Sicherheitsdienste wie Amazon GuardDuty [AWS Security Hub](#), und. AWS Config Sie können auch benutzerdefinierte Engines zur Generierung von Warnmeldungen für Sicherheitswarnungen verwenden, die nicht von diesen Diensten abgedeckt werden, oder für spezifische Warnmeldungen, die für Ihre Umgebung relevant sind. Die Erstellung dieser Warnmeldungen und Erkennungen wird in dem Abschnitt behandelt, der [the section called "Erkennung"](#) in diesem Dokument genannt wird.

Entwickeln Sie forensische Fähigkeiten

Bevor es zu einem Sicherheitsvorfall kommt, empfiehlt es sich gegebenenfalls, forensische Funktionen zur Unterstützung der Untersuchung von Sicherheitsereignissen zu entwickeln. Der [Leitfaden zur Integration forensischer Techniken in die Reaktion auf Vorfälle](#) von NIST bietet solche Anleitungen.

Forensik auf AWS

Konzepte aus der traditionellen Forensik vor Ort gelten für. AWS Die [Strategien für forensische Ermittlungsumgebungen im AWS Cloud Blogbeitrag bieten Ihnen wichtige Informationen, auf die](#) Sie bei der Migration ihrer forensischen Expertise zurückgreifen können. AWS

Sobald Sie Ihre Umgebung und AWS Kontostruktur für die Forensik eingerichtet haben, sollten Sie die Technologien definieren, die für die effektive Durchführung forensisch fundierter Methoden in den vier Phasen erforderlich sind:

- Erfassung — Sammeln Sie relevante AWS Protokolle, wie z. B. VPC Flow-Logs AWS CloudTrail und AWS Config Logs auf Hostebene. Sammeln Sie Snapshots, Backups und Speicherabbilder der betroffenen Ressourcen. AWS
- Untersuchung — Untersuchen Sie die gesammelten Daten, indem Sie die relevanten Informationen extrahieren und auswerten.
- Analyse — Analysieren Sie die gesammelten Daten, um den Vorfall zu verstehen und daraus Schlüsse zu ziehen.
- Berichterstattung — Präsentieren Sie die Informationen, die sich aus der Analysephase ergeben.

Erfassen von Backups und Snapshots

Die Einrichtung von Backups wichtiger Systeme und Datenbanken ist für die Wiederherstellung nach einem Sicherheitsvorfall und für forensische Zwecke von entscheidender Bedeutung. Mit

vorhandenen Backups können Sie Ihre Systeme wieder in einen vorherigen sicheren Zustand versetzen. Mit dieser AWS Option können Sie Schnappschüsse verschiedener Ressourcen erstellen. Mit Snapshots erhalten Sie point-in-time Backups dieser Ressourcen. Es gibt viele AWS -Services, die Sie beim Backup und der Wiederherstellung unterstützen können. Einzelheiten zu diesen Services [und Ansätzen für Backup und Recovery finden Sie in den Backup and Recovery Prescriptive Guidance](#). Weitere Informationen finden Sie im Blogbeitrag [Backups zur Wiederherstellung nach Sicherheitsvorfällen verwenden](#).

Vor allem, wenn es um Situationen wie Ransomware geht, ist es wichtig, dass Ihre Backups gut geschützt sind. Anleitungen zur [Sicherung Ihrer Backups finden Sie in den 10 besten Sicherheitsmethoden für die Sicherung von Backups im AWS](#) Blogbeitrag. Zusätzlich zum Schutz Ihrer Backups sollten Sie Ihre Backup- und Wiederherstellungsprozesse regelmäßig testen, um sicherzustellen, dass die vorhandenen Technologien und Prozesse wie erwartet funktionieren.

Automatisierung der Forensik auf AWS

Während eines Sicherheitsereignisses muss Ihr Incident-Response-Team in der Lage sein, schnell Beweise zu sammeln und zu analysieren und gleichzeitig die Genauigkeit für den Zeitraum, in dem das Ereignis stattfindet, zu gewährleisten. Für das Incident-Response-Team ist es sowohl schwierig als auch zeitaufwändig, die relevanten Beweise manuell in einer Cloud-Umgebung zu sammeln, insbesondere bei einer großen Anzahl von Instanzen und Konten. Darüber hinaus kann die manuelle Erfassung anfällig für menschliche Fehler sein. Aus diesen Gründen sollten Kunden Automatisierung für die Forensik entwickeln und implementieren.

AWS bietet eine Reihe von Automatisierungsressourcen für die Forensik, die im Anhang unter zusammengefasst sind. [the section called "Forensische Ressourcen"](#) Diese Ressourcen sind Beispiele für forensische Muster, die von entwickelt und von Kunden implementiert wurden. Obwohl sie für den Anfang eine nützliche Referenzarchitektur sein können, sollten Sie erwägen, sie zu ändern oder neue forensische Automatisierungsmuster zu erstellen, die auf Ihrer Umgebung, Ihren Anforderungen, Tools und forensischen Prozessen basieren.

Zusammenfassung der vorbereitenden Punkte

Eine gründliche Vorbereitung der Reaktion auf Sicherheitsvorfälle ist entscheidend für eine zeitnahe und effektive Reaktion auf Vorfälle. Bei der Vorbereitung der Reaktion auf Vorfälle sind Mitarbeiter, Prozesse und Technologien beteiligt. Alle drei Bereiche sind für die Vorbereitung gleich wichtig. Sie sollten Ihr Incident-Response-Programm für alle drei Bereiche vorbereiten und weiterentwickeln.

In Tabelle 2 sind die in diesem Abschnitt aufgeführten Vorbereitungspunkte zusammengefasst.

Tabelle 2 — Punkte zur Vorbereitung der Reaktion auf Vorfälle

Domain	Gegenstand der Vorbereitung	Aktionselemente
Leute	Definieren Sie Rollen und Verantwortlichkeiten.	<ul style="list-style-type: none"> • Identifizieren Sie die für die Reaktion auf Vorfälle relevanten Beteiligten. • Entwickeln Sie ein Diagramm, das verantwortlich, rechenschaftspflichtig, informiert und konsultiert RACI wurde () für einen Vorfall.
Menschen	Schulen Sie Mitarbeiter für die Reaktion auf Vorfälle darin AWS.	<ul style="list-style-type: none"> • Schulen Sie die Beteiligten bei der Reaktion auf Vorfälle auf AWS Fundamenten. • Schulen Sie die Akteure bei der Reaktion auf Vorfälle in AWS Bezug auf Sicherheits- und Überwachungsdienste. • Informieren Sie die Beteiligten bei der Reaktion auf Vorfälle über Ihre AWS Umgebung und deren Architektur.
Menschen	Verstehen Sie AWS die Support-Optionen.	<ul style="list-style-type: none"> • Machen Sie sich mit den Unterschieden in den Bereichen AWS Support, Customer Incident Response Team (CIRT), DDoS Response Team (DRT) und vertrautAMS. • Machen Sie sich mit dem Auswahlverfahren und der Eskalation vertraut, die Sie

Domain	Gegenstand der Vorbereitung	Aktionselemente
		<p>CIRT bei Bedarf während eines aktiven Sicherheitsereignisses erreichen können.</p>
Prozess	Entwickeln Sie einen Plan zur Reaktion auf Vorfälle.	<ul style="list-style-type: none"> • Erstellen Sie ein Dokument auf hoher Ebene, das Ihr Programm und Ihre Strategie zur Reaktion auf Vorfälle definiert. • Fügen Sie dem Plan zur Reaktion auf Vorfälle einen RACI Kommunikationsplan, Definitionen von Vorfällen und Phasen der Reaktion auf Vorfälle bei.
Prozess	Dokumentieren und zentralisieren Sie Architekturdiagramme.	<ul style="list-style-type: none"> • Dokumentieren Sie Einzelheiten zur Konfiguration Ihrer AWS Umgebung in Bezug auf Kontostruktur, Servicenutzung, IAM Muster und andere Kernfunktionen Ihrer AWS Konfiguration. • Entwickeln Sie Architekturdiagramme Ihrer Cloud-Architekturen.

Domain	Gegenstand der Vorbereitung	Aktionselemente
Prozess	Entwickeln Sie Playbooks zur Reaktion auf Vorfälle.	<ul style="list-style-type: none"> • Erstellen Sie eine Vorlage für die Struktur Ihrer Playbooks. • Erstellen Sie Playbooks für erwartete Sicherheitsereignisse. • Erstellen Sie Playbooks für bekannte Sicherheitswarnungen, wie z. B. GuardDuty Ergebnisse.
Prozess	Führen Sie regelmäßige Simulationen durch.	<ul style="list-style-type: none"> • Entwickeln Sie einen regelmäßigen Rhythmus, um Vorfallsimulationen durchzuführen. • Nutzen Sie die Ergebnisse und gewonnenen Erkenntnisse, um Ihr Programm zur Reaktion auf Vorfälle weiterzuentwickeln.
Technologie	Entwickeln Sie eine AWS Kontostruktur.	<ul style="list-style-type: none"> • Planen Sie eine Kontostruktur, in der festgelegt ist, wie Workloads nach AWS Konten getrennt werden. • Erstellen Sie eine Sicherheits-OU mit einem Sicherheitstool und einem Konto für die Protokollarchivierung. • Erstellen Sie eine forensische Organisationseinheit mit forensischen Konten für jede Region, in der Sie tätig sind.

Domain	Gegenstand der Vorbereitung	Aktionselemente
Technologie	Entwickeln und implementieren Sie eine Tagging-Strategie, die es den Einsatzkräften ermöglicht, die Verantwortung und den Kontext der Ergebnisse zu identifizieren.	<ul style="list-style-type: none"> • Planen Sie eine Strategie für das Tagging und welche Tags Sie mit Ihren Ressourcen verknüpfen möchten. AWS • Implementieren Sie die Tagging-Strategie und setzen Sie sie durch.
Technologie	Kontaktinformationen für das AWS Konto aktualisieren.	<ul style="list-style-type: none"> • Vergewissern Sie sich, dass AWS für die Konten Kontaktinformationen aufgeführt sind. • Erstellen Sie E-Mail-Verteilerlisten für die Kontaktinformationen, um einzelne Fehlerquellen zu vermeiden. • Schützen Sie die E-Mail-Konten, die mit den AWS Kontoinformationen verknüpft sind.
Technologie	Bereiten Sie den Zugriff auf AWS Konten vor.	<ul style="list-style-type: none"> • Definieren Sie, welchen Zugriff Incident-Responder benötigen, um auf einen Vorfall zu reagieren. • Implementieren, testen und überwachen Sie den Zugriff.

Domain	Gegenstand der Vorbereitung	Aktionselemente
Technologie	Verstehen Sie die Bedrohungslandschaft.	<ul style="list-style-type: none"> • Entwickeln Sie Bedrohungsmodelle für Ihre Umgebung und Anwendungen. • Integrieren und nutzen Sie Informationen zu Cyberbedrohungen.
Technologie	Wählen Sie Protokolle aus und richten Sie sie ein.	<ul style="list-style-type: none"> • Identifizieren und aktivieren Sie Protokolle für Untersuchungen. • Wählen Sie Protokollspeicher aus. • Identifizieren und implementieren Sie die Protokollaufbewahrung. • Entwickeln Sie einen Mechanismus zum Abrufen und Abfragen von Protokollen und Artefakten. • Verwenden Sie Protokolle für Warnmeldungen.
Technologie	Entwickeln Sie forensische Fähigkeiten.	<ul style="list-style-type: none"> • Identifizieren Sie Artefakte, die für die forensische Erfassung erforderlich sind. • Erfassen und sichern Sie Backups wichtiger Systeme. • Definieren Sie Mechanismen für die Analyse identifizierter Logs und Artefakte. • Implementieren Sie Automatisierung für forensische Analysen.

Für die Vorbereitung der Reaktion auf Vorfälle wird ein iterativer Ansatz empfohlen. All diese Vorbereitungsschritte können nicht über Nacht erledigt werden. Sie sollten einen Plan erstellen, um klein anzufangen und Ihre Fähigkeiten zur Reaktion auf Vorfälle im Laufe der Zeit kontinuierlich zu verbessern.

Operationen

Der Betrieb ist der Kern der Reaktion auf Vorfälle. Hier finden die Maßnahmen zur Reaktion und Behebung von Sicherheitsvorfällen statt. Der Betrieb umfasst die folgenden fünf Phasen: Erkennung, Analyse, Eindämmung, Beseitigung und Wiederherstellung. Eine Beschreibung dieser Phasen und der Ziele finden Sie in Tabelle 3.

Tabelle 3 — Betriebsphasen

Phase	Ziel
Erkennung	Identifizieren eines potenziellen Sicherheitsereignisses.
Analyse	Stellen Sie fest, ob es sich bei einem Sicherheitsereignis um einen Vorfall handelt, und beurteilen Sie den Umfang des Vorfalls.
Eindämmung	Minimieren und Beschränken des Umfangs des Sicherheitsereignisses.
Ausrottung	Entfernen nicht autorisierter Ressourcen oder Artefakte im Zusammenhang mit dem Sicherheitsereignis. Implementieren von Abhilfemaßnahmen zur Behebung der Ursache des Sicherheitsvorfalls.
Erholung	Stellen Sie die Systeme in einen bekannten sicheren Zustand zurück und überwachen Sie diese Systeme, um sicherzustellen, dass die Bedrohung nicht erneut auftritt.

Die Phasen sollen als Leitfaden für die Reaktion auf Sicherheitsvorfälle und deren Behandlung dienen, damit Sie effektiv und nachhaltig reagieren können. Die tatsächlichen Maßnahmen, die Sie ergreifen, sind abhängig vom jeweiligen Vorfall. Bei einem Vorfall mit Ransomware müssen beispielsweise andere Schritte ausgeführt werden als bei einem Vorfall, an dem ein öffentlicher Amazon-S3-Bucket beteiligt ist. Darüber hinaus folgen diese Phasen nicht unbedingt aufeinander. Nach der Eindämmung und Beseitigung müssen Sie möglicherweise zur Analyse zurückkehren, um zu ermitteln, ob Ihre Maßnahmen wirksam waren.

Erkennung

Eine Warnung ist der Hauptbestandteil der Erkennungsphase. Sie generiert eine Benachrichtigung, um den Prozess zur Reaktion auf Vorfälle auf der Grundlage der AWS gewünschten Kontoaktivität einzuleiten.

Die Genauigkeit von Warnmeldungen ist eine Herausforderung. Es ist nicht immer möglich, mit absoluter Sicherheit zu bestimmen, ob ein Vorfall eingetreten ist, im Gange ist oder ob er in future passieren wird. Hier sind ein paar Gründe:

- Erkennungsmechanismen basieren auf Basisabweichungen, bekannten Mustern und Benachrichtigungen von internen oder externen Stellen.
- Aufgrund der Unvorhersehbarkeit der Technologie und der Menschen bzw. der Mittel und Akteure von Sicherheitsvorfällen ändern sich die Ausgangswerte im Laufe der Zeit. Durch neuartige oder modifizierte Taktiken, Techniken und Verfahren der Bedrohungsakteure entstehen böartige Muster (). TTPs
- Änderungen an Mitarbeitern, Technologien und Prozessen werden nicht sofort in den Prozess zur Reaktion auf Vorfälle integriert. Einige werden im Verlauf einer Untersuchung entdeckt.

Quellen der Warnung

Sie sollten erwägen, die folgenden Quellen zur Definition von Warnmeldungen zu verwenden:

- Ergebnisse — AWS Dienste wie [Amazon GuardDuty](#), [Amazon Macie](#) [AWS Security Hub](#), [Amazon Inspector](#) [AWS Config](#), [IAMAccess Analyzer](#) und [Network Access Analyzer](#) generieren Ergebnisse, die zur Erstellung von Warnmeldungen verwendet werden können.
- Protokolle — AWS Service-, Infrastruktur- und Anwendungsprotokolle, die in Amazon S3 S3-Buckets und CloudWatch Protokollgruppen gespeichert sind, können analysiert und korreliert werden, um Warnmeldungen zu generieren.

- **Abrechnungsaktivität** — Eine plötzliche Änderung der Abrechnungsaktivität kann auf ein Sicherheitsereignis hinweisen. Folgen Sie der Dokumentation unter [Einrichtung eines Fakturierungsalarms zur Überwachung Ihrer geschätzten AWS Gebühren](#), um dies zu überprüfen.
- **Informationen zu Cyberbedrohungen** — Wenn Sie einen Feed mit Informationen zu Cyberbedrohungen eines Drittanbieters abonnieren, können Sie diese Informationen mit anderen Protokollierungs- und Überwachungstools korrelieren, um potenzielle Indikatoren für Ereignisse zu identifizieren.
- **Partner-Tools** — Partner in AWS Partner Network (APN) bieten erstklassige Produkte, mit denen Sie Ihre Sicherheitsziele erreichen können. Für die Reaktion auf Vorfälle können Partnerprodukte mit Endpoint Detection and Response (EDR) eingesetzt werden oder Sie SIEM können Sie bei der Unterstützung Ihrer Ziele bei der Reaktion auf Vorfälle unterstützen. Weitere Informationen finden Sie unter [Sicherheitspartnerlösungen](#) und [Sicherheitslösungen im AWS Marketplace](#).
- **AWS Vertrauen und Sicherheit** — Wir Support könnten uns an Kunden wenden, wenn wir missbräuchliche oder böswillige Aktivitäten feststellen.
- **Einmaliger Kontakt** — Da es Ihre Kunden, Entwickler oder andere Mitarbeiter in Ihrem Unternehmen sein können, denen etwas Ungewöhnliches auffällt, ist es wichtig, dass Sie Ihr Sicherheitsteam über eine bekannte und gut bekannt gewordene Methode kontaktieren. Zu den beliebtesten Optionen gehören Ticketsysteme, Kontakt-E-Mail-Adressen und Webformulare. Wenn Ihre Organisation mit der breiten Öffentlichkeit zusammenarbeitet, benötigen Sie möglicherweise auch einen Sicherheitsmechanismus für die Öffentlichkeit.

Weitere Informationen zu Cloud-Funktionen, die Sie bei Ihren Untersuchungen nutzen können, finden Sie [the section called “Anhang A: Definitionen der Cloud-Funktionen”](#) in diesem Dokument.

Erkennung als Teil der Sicherheitskontrolltechnik

Erkennungsmechanismen sind ein integraler Bestandteil der Entwicklung der Sicherheitskontrolle. Sobald Richtlinien und präventive Kontrollen definiert sind, sollten entsprechende detektive und reaktive Kontrollen eingeführt werden. Beispielsweise richtet eine Organisation eine Direktive für den Root-Benutzer eines AWS Kontos ein, die nur für bestimmte und sehr genau definierte Aktivitäten verwendet werden sollte. Sie verbinden sie mit einer präventiven Kontrolle, die mithilfe der Dienstkontrollrichtlinie (SCP) einer AWS Organisation implementiert wird. Wenn Root-Benutzeraktivitäten über den erwarteten Basiswert hinausgehen, alarmiert eine mit einer EventBridge Regel und einem SNS Thema implementierte Detective Control das Security Operations Center (SOC). Die reaktionsschnelle Kontrolle umfasst die SOC Auswahl des geeigneten Playbooks, die Durchführung von Analysen und die Arbeit, bis der Vorfall behoben ist.

Sicherheitskontrollen lassen sich am besten anhand der Bedrohungsmodellierung der laufenden Workloads definieren. AWS Die Wichtigkeit detektiver Kontrollen wird anhand der Geschäftsauswirkungsanalyse (BIA) für die jeweilige Arbeitslast festgelegt. Durch detektivische Kontrollen ausgelöste Warnmeldungen werden nicht sofort bearbeitet, sondern auf der Grundlage ihrer anfänglichen Kritikalität, die im Laufe der Analyse angepasst werden muss. Die Festlegung der anfänglichen Kritikalität dient als Hilfe bei der Priorisierung. Der Kontext, in dem die Warnung ausgelöst wurde, bestimmt ihre tatsächliche Kritikalität. Ein Beispiel: Eine Organisation verwendet Amazon GuardDuty als Bestandteil der detektiven Kontrolle, die für EC2 Instances verwendet wird, die Teil eines Workloads sind. Das Ergebnis `Impact:EC2/SuspiciousDomainRequest.Reputation` wird generiert und informiert Sie darüber, dass die aufgelistete EC2 Amazon-Instance in Ihrem Workload einen Domainnamen abfragt, bei dem der Verdacht besteht, dass er bösartig ist. Diese Warnung ist standardmäßig auf einen niedrigen Schweregrad eingestellt. Im Verlauf der Analysephase wurde festgestellt, dass mehrere hundert EC2 Instanzen dieses Typs von einem nicht autorisierten Akteur bereitgestellt wurden, was die Betriebskosten des Unternehmens erheblich in die Höhe trieb. Zu diesem Zeitpunkt trifft das Incident-Response-Team die Entscheidung, die Kritikalität dieser Warnung auf hoch zu setzen, wodurch das Gefühl der Dringlichkeit verstärkt und weitere Maßnahmen beschleunigt werden. Beachten Sie, dass der Schweregrad des GuardDuty Befundes nicht geändert werden kann.

Implementierungen von Detective Control

Es ist wichtig zu verstehen, wie Detective Controls implementiert werden, da sie dazu beitragen, zu bestimmen, wie die Warnung für ein bestimmtes Ereignis verwendet wird. Es gibt zwei Hauptimplementierungen von technischen Detektivkontrollen:

- Die Verhaltenserkennung basiert auf mathematischen Modellen, die allgemein als maschinelles Lernen (ML) oder künstliche Intelligenz (KI) bezeichnet werden. Die Erkennung erfolgt durch Inferenz. Daher spiegelt die Warnung möglicherweise nicht unbedingt ein aktuelles Ereignis wider.
- Die regelbasierte Erkennung ist deterministisch. Kunden können die genauen Parameter dafür festlegen, bei welcher Aktivität gewarnt werden soll, und das ist sicher.

Moderne Implementierungen von Erkennungssystemen, wie z. B. ein Einbruchmeldesystem (IDS), verfügen in der Regel über beide Mechanismen. Im Folgenden finden Sie einige Beispiele für regelbasierte und verhaltensbasierte Erkennungen mit GuardDuty

- Wenn das Ergebnis generiert `Exfiltration:IAMUser/AnomalousBehavior` wird, werden Sie darüber informiert, dass „in Ihrem Konto eine ungewöhnliche API Anfrage festgestellt wurde“. Wenn Sie sich die Dokumentation genauer ansehen, erfahren Sie, dass „das ML-Modell alle API

Anfragen in Ihrem Konto bewertet und ungewöhnliche Ereignisse identifiziert, die mit den von Gegnern verwendeten Techniken in Verbindung stehen“, was darauf hindeutet, dass es sich bei diesem Befund um verhaltensbedingte Ergebnisse handelt.

- Zu diesem Ergebnis `Impact:S3/MaliciousIPCaller` werden API Anrufe vom Amazon S3 S3-Service analysiert und das `SourceIPAddress` Protokollelement mit einer Tabelle mit öffentlichen IP-Adressen verglichen CloudTrail, die Feeds mit Bedrohungsinformationen enthält. GuardDuty Sobald es eine direkte Übereinstimmung mit einem Eintrag findet, generiert es das Ergebnis.

Wir empfehlen die Implementierung einer Mischung aus verhaltensbasierten und regelbasierten Warnmeldungen, da es nicht immer möglich ist, regelbasierte Warnmeldungen für jede Aktivität innerhalb Ihres Bedrohungsmodells zu implementieren.

Personengestützte Erkennung

Bis zu diesem Zeitpunkt haben wir über technologiegestützte Erkennung gesprochen. Die andere wichtige Erkennungsquelle sind Personen innerhalb oder außerhalb der Organisation des Kunden. Insider können als Mitarbeiter oder Auftragnehmer definiert werden, und Außenstehende sind Entitäten wie Sicherheitsforscher, Strafverfolgungsbehörden, Nachrichtendienste und soziale Medien.

Obwohl die technologiegestützte Erkennung systematisch konfiguriert werden kann, gibt es eine Vielzahl von Formen, wie z. B. E-Mails, Tickets, Post, Nachrichtenbeiträge, Telefonanrufe und persönliche Interaktionen. Es kann davon ausgegangen werden, dass technologiegestützte Erkennungsbenachrichtigungen nahezu in Echtzeit zugestellt werden, es gibt jedoch keine Zeitvorgaben für die Erkennung durch Personen. Es ist unerlässlich, dass die Sicherheitskultur personengestützte Erkennungsmechanismen einbezieht, erleichtert und unterstützt, um einen umfassenden Sicherheitsansatz zu gewährleisten.

Übersicht

Bei der Erkennung ist es wichtig, eine Mischung aus regelbasierten und verhaltensorientierten Warnmeldungen zu haben. Darüber hinaus sollten Sie über Mechanismen verfügen, mit denen interne und externe Personen ein Ticket zu einem Sicherheitsproblem einreichen können. Menschen können eine der wertvollsten Quellen für Sicherheitsereignisse sein. Daher ist es wichtig, über Prozesse zu verfügen, mit denen Menschen Bedenken äußern können. Sie sollten die Bedrohungsmodelle Ihrer Umgebung verwenden, um mit der Erkennung von Gebäuden zu beginnen. Mithilfe von Bedrohungsmodellen können Sie Warnmeldungen erstellen, die auf Bedrohungen basieren, die für Ihre Umgebung am relevantesten sind. Schließlich können Sie Frameworks wie MITRE ATT &CK verwenden, um die Taktiken, Techniken und Verfahren von Bedrohungsakteuren zu

verstehen (TTPs). Es kann hilfreich sein, das MITRE ATT &CK-Framework als gemeinsame Sprache für Ihre verschiedenen Erkennungsmechanismen zu verwenden.

Analyse

Protokolle, Abfragefunktionen und Bedrohungsinformationen sind nur einige der unterstützenden Komponenten, die für die Analysephase erforderlich sind. Viele der zur Erkennung verwendeten Protokolle werden auch für Analysen verwendet und erfordern das Onboarding und die Konfiguration von Abfragetools.

Validierung, Umfang und Bewertung der Auswirkungen der Warnung

Während der Analysephase wird eine umfassende Protokollanalyse mit dem Ziel durchgeführt, Warnmeldungen zu validieren, den Umfang zu definieren und die Auswirkungen einer möglichen Gefährdung zu bewerten.

- Die Validierung der Warnung ist der Ausgangspunkt der Analysephase. Incident-Responder werden nach Protokolleinträgen aus verschiedenen Quellen suchen und sich direkt mit den Eigentümern der betroffenen Workloads in Verbindung setzen.
- Die Festlegung des Geltungsbereichs ist der nächste Schritt, bei dem alle beteiligten Ressourcen inventarisiert und die Kritikalität der Warnmeldungen angepasst wird, nachdem sich die Beteiligten einig sind, dass es sich wahrscheinlich nicht um ein falsches Positivsignal handelt.
- Schließlich wird in der Folgenabschätzung die tatsächliche Betriebsstörung detailliert beschrieben.

Sobald die betroffenen Workload-Komponenten identifiziert sind, können die Ergebnisse des Scopings mit den Zielen für den Wiederherstellungspunkt (RPO) und der Wiederherstellungszeit () des jeweiligen Workloads korreliert werden. Dabei wird die Kritikalität der Warnmeldungen berücksichtigt, wodurch die Ressourcenzuweisung und alle weiteren Aktivitäten eingeleitet werden. RTO Nicht alle Vorfälle beeinträchtigen unmittelbar den Betrieb eines Workloads, der einen Geschäftsprozess unterstützt. Vorfälle wie die Offenlegung vertraulicher Daten, der Diebstahl geistigen Eigentums oder die Entführung von Ressourcen (wie beim Mining von Kryptowährungen) können einen Geschäftsprozess möglicherweise nicht sofort stoppen oder schwächen, können jedoch zu einem späteren Zeitpunkt Konsequenzen haben.

Reichern Sie Sicherheitsprotokolle und Ergebnisse an

Bereicherung mit Bedrohungsinformationen und organisatorischem Kontext

Im Laufe der Analyse müssen die interessierenden Observablen angereichert werden, um die Warnung besser kontextualisieren zu können. Wie im Abschnitt Vorbereitung beschrieben, kann die Integration und Nutzung von Informationen über Cyberbedrohungen hilfreich sein, um mehr über eine Sicherheitsfeststellung zu erfahren. Threat Intelligence Services werden verwendet, um öffentlichen IP-Adressen, Domainnamen und Datei-Hashes Reputation und Eigentumsrechte zuzuweisen. Diese Tools sind als kostenpflichtige und als kostenlose Dienste erhältlich.

Kunden, die Amazon Athena als Tool zur Protokollabfrage verwenden, profitieren von den Vorteilen von AWS Glue-Jobs, um Bedrohungsinformationen als Tabellen zu laden. Die Threat-Intelligence-Tabellen können in SQL Abfragen verwendet werden, um Protokollelemente wie IP-Adressen und Domainnamen zu korrelieren und so eine erweiterte Ansicht der zu analysierenden Daten zu erhalten.

AWS GuardDuty stellt Kunden keine Bedrohungsinformationen direkt zur Verfügung, aber Dienste wie Amazon nutzen Bedrohungsinformationen zur Anreicherung und Generierung von Erkenntnissen. Sie können auch benutzerdefinierte Bedrohungslisten hochladen, die auf Ihren eigenen Bedrohungsinformationen GuardDuty basieren.

Bereicherung durch Automatisierung

Automatisierung ist ein integraler Bestandteil der AWS Cloud Unternehmensführung. Sie kann in den verschiedenen Phasen des Incident-Response-Lebenszyklus eingesetzt werden.

In der Erkennungsphase gleicht die regelbasierte Automatisierung anhand von Protokollen die für das Bedrohungsmodell relevanten Muster ab und ergreift geeignete Maßnahmen, z. B. das Senden von Benachrichtigungen. In der Analysephase kann der Erkennungsmechanismus genutzt und die Warnmeldung an eine Engine weitergeleitet werden, die in der Lage ist, Protokolle abzufragen und Observables zur Kontextualisierung des Ereignisses anzureichern.

Die Warnstelle besteht in ihrer grundlegenden Form aus einer Ressource und einer Identität. Beispielsweise könnten Sie eine Automatisierung implementieren, um nach AWS API Aktivitäten abzufragen CloudTrail, die von der Identität oder Ressource der Warnstelle rund um den Zeitpunkt der Warnung ausgeführt wurden, wodurch zusätzliche Erkenntnisse wie `eventSource`, `eventNameSourceIPAddress`, und `userAgent` identifizierte API Aktivitäten bereitgestellt werden. Durch die automatisierte Ausführung dieser Abfragen können die Responder Zeit bei der Triage sparen und zusätzlichen Kontext erhalten, um fundiertere Entscheidungen zu treffen.

Im Blogbeitrag [Wie man AWS Security Hub Hub-Ergebnisse mit Konto-Metadaten anreichert](#), finden Sie ein Beispiel dafür, wie Sie mithilfe von Automatisierung Sicherheitsergebnisse anreichern und Analysen vereinfachen können.

Sammeln und analysieren Sie forensische Beweise

Forensik ist, wie im [the section called "Vorbereitung"](#) Abschnitt dieses Dokuments erwähnt, der Prozess der Erfassung und Analyse von Artefakten bei der Reaktion auf Vorfälle. On AWS ist auf Infrastrukturdomänenressourcen wie die Erfassung von Netzwerkdatenverkehrspaketen, Speicherabbilder des Betriebssystems und für Dienstdomänenressourcen wie Protokolle anwendbar. AWS CloudTrail

Der forensische Prozess weist die folgenden grundlegenden Merkmale auf:

- Konsistent — Er folgt exakt den dokumentierten Schritten, ohne Abweichungen.
- Wiederholbar — Es führt zu exakt den gleichen Ergebnissen, wenn es gegen dasselbe Artefakt wiederholt wird.
- Üblich — Es ist öffentlich dokumentiert und weit verbreitet.

Es ist wichtig, dass für Artefakte, die bei der Reaktion auf Vorfälle gesammelt wurden, eine Kontrollkette eingehalten wird. Neben der Speicherung der Artefakte in schreibgeschützten Repositories können Automatisierung und die automatische Erstellung einer Dokumentation dieser Sammlung hilfreich sein. Die Analyse sollte nur an exakten Replikaten der gesammelten Artefakte durchgeführt werden, um die Integrität zu wahren.

Sammeln Sie relevante Artefakte

Unter Berücksichtigung dieser Merkmale und auf der Grundlage der entsprechenden Warnmeldungen und der Bewertung der Auswirkungen und des Umfangs müssen Sie die Daten sammeln, die für weitere Untersuchungen und Analysen relevant sind. Verschiedene Arten und Quellen von Daten, die für eine Untersuchung relevant sein könnten, darunter Protokolle der Service- und Kontrollebene (CloudTrail, Amazon S3 S3-Datenereignisse, VPC Flow Logs), Daten (Amazon S3 S3-Metadaten und -Objekte) und Ressourcen (Datenbanken, EC2 Amazon-Instances).

Protokolle der Service- und Kontrollebene können für lokale Analysen gesammelt oder idealerweise direkt über native AWS Dienste (falls zutreffend) abgefragt werden. Daten (einschließlich Metadaten) können direkt abgefragt werden, um relevante Informationen zu erhalten oder die Quellobjekte abzurufen. Verwenden Sie beispielsweise die AWS CLI um Amazon S3 S3-Bucket- und Objektmetadaten abzurufen und Quellobjekte direkt abzurufen. Ressourcen müssen auf eine Weise

gesammelt werden, die dem Ressourcentyp und der beabsichtigten Analysemethode entspricht. Datenbanken können beispielsweise gesammelt werden, indem eine copy/snapshot of the system running the database, creating a copy/snapshot der gesamten Datenbank selbst erstellt wird oder bestimmte Daten und Protokolle aus der Datenbank abgefragt und extrahiert werden, die für die Untersuchung relevant sind.

Für EC2 Amazon-Instances gibt es einen bestimmten Datensatz, der gesammelt werden sollte, und eine bestimmte Reihenfolge der Erfassung, die durchgeführt werden sollte, um die größtmögliche Menge an Daten für Analysen und Untersuchungen zu erfassen und zu speichern.

Konkret lautet die Reihenfolge für Response, um die meisten Datenmengen von einer EC2 Amazon-Instance zu erfassen und zu speichern, wie folgt:

1. Instance-Metadaten abrufen — Erfassen Sie Instance-Metadaten, die für die Untersuchung und Datenabfragen relevant sind (Instance-ID, Typ, IP-Adresse, VPC /Subnetz-ID, Region, Amazon Machine Image (AMI) -ID, angehängte Sicherheitsgruppen, Startzeit).
2. Instanzschutz und Tags aktivieren — Aktivieren Sie Instanzschutzmaßnahmen wie Kündigungsschutz, Einstellung des Shutdown-Verhaltens auf Stopp (falls auf Beenden gesetzt), Deaktivieren von Delete on Termination-Attributen für die angehängten EBS Volumes und Anwenden geeigneter Tags sowohl für die visuelle Kennzeichnung als auch für die Verwendung in möglichen Reaktionsautomatisierungen (z. B. beim Anwenden eines Tags mit dem Namen Status und Wert von `Quarantine`, führen Sie eine forensische Erfassung von Daten durch und isolieren Sie die Instanz).
3. Festplatte abrufen (EBSSnapshots) — Erfassen Sie einen EBS Snapshot der angehängten EBS Volumes. Jeder Snapshot enthält die Informationen, die Sie benötigen, um Ihre Daten (ab dem Zeitpunkt, an dem der Snapshot erstellt wurde) auf einem neuen EBS Volume wiederherzustellen. Sehen Sie sich den Schritt zur Live-Erfassung von Antworten/Artefakten an, wenn Sie Instance-Speicher-Volumes verwenden.
4. Arbeitsspeicher abrufen — Da EBS Snapshots nur Daten erfassen, die auf Ihr EBS Amazon-Volume geschrieben wurden, was Daten ausschließen kann, die von Ihren Anwendungen oder Ihrem Betriebssystem im Speicher gespeichert oder zwischengespeichert werden, ist es unerlässlich, ein Systemspeicher-Image mithilfe eines geeigneten Open-Source-Tools oder kommerziellen Tools eines Drittanbieters zu erwerben, um verfügbare Daten aus dem System abzurufen.
5. (Optional) Live-Antwort-/Artefakterfassung durchführen — Führen Sie eine gezielte Datenerfassung (disk/memory/logs) über Live-Response auf dem System nur durch, wenn Festplatte oder Arbeitsspeicher nicht anderweitig abgerufen werden können oder wenn ein triftiger

geschäftlicher oder betrieblicher Grund vorliegt. Dadurch werden wertvolle Systemdaten und Artefakte verändert.

6. Instance außer Betrieb nehmen — Trennen Sie die Instance von Auto Scaling Scaling-Gruppen, heben Sie die Registrierung der Instance bei Load Balancers auf und passen Sie ein vorgefertigtes Instance-Profil mit minimierten oder keinen Berechtigungen an oder wenden Sie es an.
7. Instanz isolieren oder eindämmen — Stellen Sie sicher, dass die Instanz effektiv von anderen Systemen und Ressourcen in der Umgebung isoliert ist, indem Sie aktuelle und future Verbindungen zu und von der Instance beenden und verhindern. Weitere Informationen finden Sie [the section called “Eindämmung”](#) im Abschnitt dieses Dokuments.
8. Wahl des Responders — Wählen Sie je nach Situation und Zielen eine der folgenden Optionen aus:
 - Das System außer Betrieb nehmen und herunterfahren (empfohlen).

Schalten Sie das System ab, sobald die verfügbaren Beweise vorliegen, um zu überprüfen, wie die Instanz am wirksamsten gegen mögliche future Auswirkungen auf die Umwelt vorbeugen kann.

- Führen Sie die Instance weiterhin in einer isolierten Umgebung aus, die für die Überwachung instrumentiert ist.

Es wird zwar nicht als Standardansatz empfohlen, aber wenn eine Situation eine kontinuierliche Beobachtung der Instance erfordert (z. B. wenn zusätzliche Daten oder Indikatoren für eine umfassende Untersuchung und Analyse der Instance benötigt werden), können Sie erwägen, die Instance herunterzufahren, eine AMI der Instance zu erstellen und die Instance in Ihrem speziellen Forensik-Konto in einer Sandbox-Umgebung neu zu starten, die so vorkonfiguriert ist, dass sie vollständig isoliert und mit Instrumentierung konfiguriert ist, um eine nahezu kontinuierliche Überwachung der Instance zu ermöglichen (zum Beispiel VPC Flow Logs oder VPC Traffic Mirroring).

Note

Um verfügbare flüchtige (und wertvolle) Daten zu erfassen, ist es wichtig, den Arbeitsspeicher vor Live-Reaktionsaktivitäten oder Systemisolierung oder Systemabschaltung zu erfassen.

Entwickeln Sie Erzählungen

Dokumentieren Sie während der Analyse und Untersuchung die ergriffenen Maßnahmen, die durchgeführten Analysen und die identifizierten Informationen, die in den nachfolgenden Phasen und schließlich in einem Abschlussbericht verwendet werden können. Diese Schilderungen sollten kurz und präzise sein und bestätigen, dass relevante Informationen enthalten sind, um ein effektives Verständnis des Vorfalls zu gewährleisten und einen genauen Zeitplan einzuhalten. Sie sind auch hilfreich, wenn Sie Personen außerhalb des Kernteams für die Reaktion auf Vorfälle einbeziehen. Ein Beispiel:

i Die Marketing- und Vertriebsabteilung erhielt am 15. März 2022 eine Lösegeldforderung, in der die Zahlung in Kryptowährung gefordert wurde, um die öffentliche Veröffentlichung möglicher sensibler Daten zu verhindern. Die SOC stellten fest, dass die zu Marketing und Vertrieb gehörende RDS Amazon-Datenbank am 20. Februar 2022 öffentlich zugänglich war. Die SOC wurden RDS Zugriffsprotokolle abgefragt und festgestellt, dass die IP-Adresse 198.51.100.23 am 20. Februar 2022 mit den Anmeldeinformationen von Major Mary, einem der `mm03434` Webentwickler, verwendet wurde. Die SOC abgefragten VPC Flow Logs stellten fest, dass ungefähr 256 MB an Daten am selben Tag an dieselbe IP-Adresse übertragen wurden (Zeitstempel 2022-02-20T 15:50 +00Z). Sie haben anhand von Open-Source-Bedrohungsinformationen SOC festgestellt, dass die Anmeldeinformationen derzeit im Klartext im öffentlichen Repository verfügbar sind. `https[:]//example[.]com/majormary/rds-utils`

Eindämmung

Eine Definition von Eindämmung in Bezug auf die Reaktion auf Vorfälle ist der Prozess oder die Implementierung einer Strategie bei der Behandlung eines Sicherheitsereignisses, die darauf abzielt, den Umfang des Sicherheitsereignisses zu minimieren und die Auswirkungen einer unbefugten Nutzung innerhalb der Umgebung einzudämmen.

Eine Eindämmungsstrategie hängt von einer Vielzahl von Faktoren ab und kann sich von Organisation zu Organisation in Bezug auf die Anwendung der Eindämmungstaktiken, den Zeitpunkt und den Zweck unterscheiden. Der [NISTSP 800-61 Leitfaden zur Behandlung von Computersicherheitsvorfällen](#) beschreibt mehrere Kriterien für die Bestimmung der geeigneten Eindämmungsstrategie, darunter:

- Mögliche Beschädigung und Diebstahl von Ressourcen

- Notwendigkeit der Beweissicherung
- Verfügbarkeit von Diensten (Netzwerkonnektivität, für externe Parteien bereitgestellte Dienste)
- Zeit und Ressourcen, die für die Umsetzung der Strategie benötigt wurden
- Wirksamkeit der Strategie (teilweise oder vollständige Eindämmung)
- Dauer der Lösung (Notfalllösung muss innerhalb von vier Stunden entfernt werden, vorübergehende Behelfslösung muss in zwei Wochen entfernt werden, permanente Lösung)

Hinsichtlich der verfügbaren AWS Dienste lassen sich die grundlegenden Maßnahmen zur Eindämmung jedoch in drei Kategorien unterteilen:

- Eingrenzung von Quellen — Verwenden Sie Filter und Routing, um den Zugriff von einer bestimmten Quelle aus zu verhindern.
- Technik und Zugriffskontrolle — Sperren Sie den Zugriff, um unbefugten Zugriff auf die betroffenen Ressourcen zu verhindern.
- Zieleindämmung — Verwenden Sie Filterung und Routing, um den Zugriff auf eine Zielressource zu verhindern.

Quell-Containment

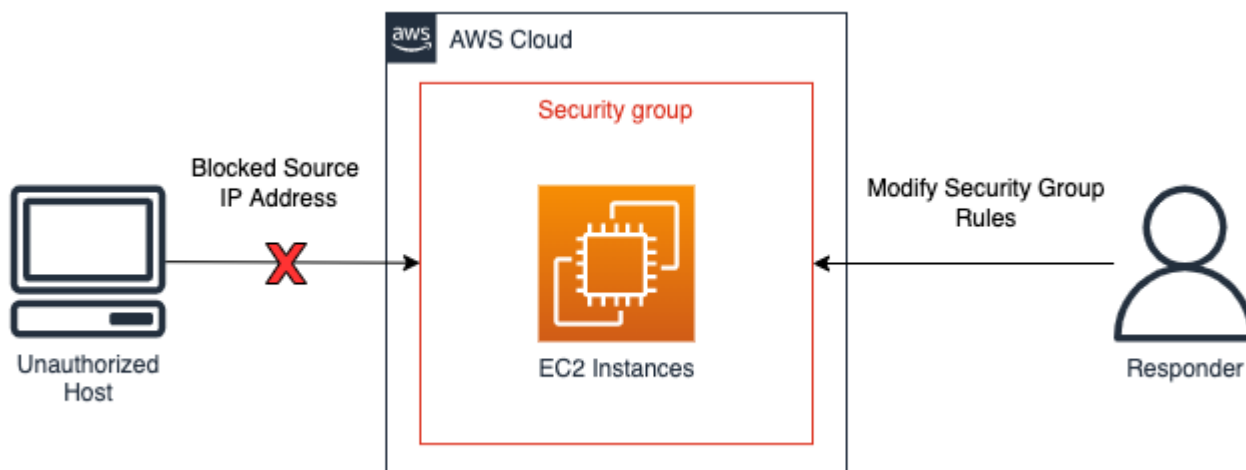
Quelleneinhausung ist die Verwendung und Anwendung von Filtern oder Routing innerhalb einer Umgebung, um den Zugriff auf Ressourcen von einer bestimmten Quell-IP-Adresse oder einem bestimmten Netzwerkbereich aus zu verhindern. Beispiele für die Eingrenzung von Quellen mithilfe von AWS Diensten werden hier hervorgehoben:

- Sicherheitsgruppen — Das Erstellen und Anwenden isolierter Sicherheitsgruppen auf EC2 Amazon-Instances oder das Entfernen von Regeln aus einer vorhandenen Sicherheitsgruppe kann dazu beitragen, unbefugten Datenverkehr zu einer EC2 Amazon-Instance oder AWS -Ressource einzudämmen. Es ist wichtig zu beachten, dass bestehende nachverfolgte Verbindungen nicht aufgrund wechselnder Sicherheitsgruppen geschlossen werden — nur future Datenverkehr wird von der neuen Sicherheitsgruppe effektiv blockiert (weitere Informationen zu verfolgten und nicht verfolgten Verbindungen finden Sie in [diesem Incident Response Playbook](#) und in der [Verbindungsverfolgung von Sicherheitsgruppen](#)).
- Richtlinien — Amazon S3 S3-Bucket-Richtlinien können so konfiguriert werden, dass sie Datenverkehr von einer IP-Adresse, einem Netzwerkbereich oder einem VPC Endpunkt blockieren oder zulassen. Richtlinien ermöglichen es, verdächtige Adressen und den Zugriff auf den Amazon

S3 S3-Bucket zu blockieren. Weitere Informationen zu Bucket-Richtlinien finden Sie unter [Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole](#).

- AWS WAF — Web-Zugriffskontrolllisten (WebACLs) können konfiguriert werden AWS WAF , um eine detaillierte Kontrolle über Webanfragen zu ermöglichen, auf die Ressourcen antworten. Sie können einem IP-Set, für das konfiguriert ist AWS WAF, eine IP-Adresse oder einen Netzwerkbereich hinzufügen und Vergleichsbedingungen wie Sperren auf den IP-Satz anwenden. Dadurch werden Webanfragen an eine Ressource blockiert, wenn die IP-Adresse oder die Netzwerkbereiche des ursprünglichen Datenverkehrs mit den in den IP-Set-Regeln konfigurierten Bereichen übereinstimmen.

Ein Beispiel für die Eindämmung von Quellen ist in der folgenden Abbildung zu sehen. Ein Incident-Response-Analyst ändert eine Sicherheitsgruppe einer EC2 Amazon-Instance, um neue Verbindungen nur auf bestimmte IP-Adressen zu beschränken. Wie im Aufzähler Sicherheitsgruppen angegeben, werden bestehende nachverfolgte Verbindungen nicht aufgrund von Änderungen der Sicherheitsgruppen heruntergefahren.



Beispiel für eine Quellensperre

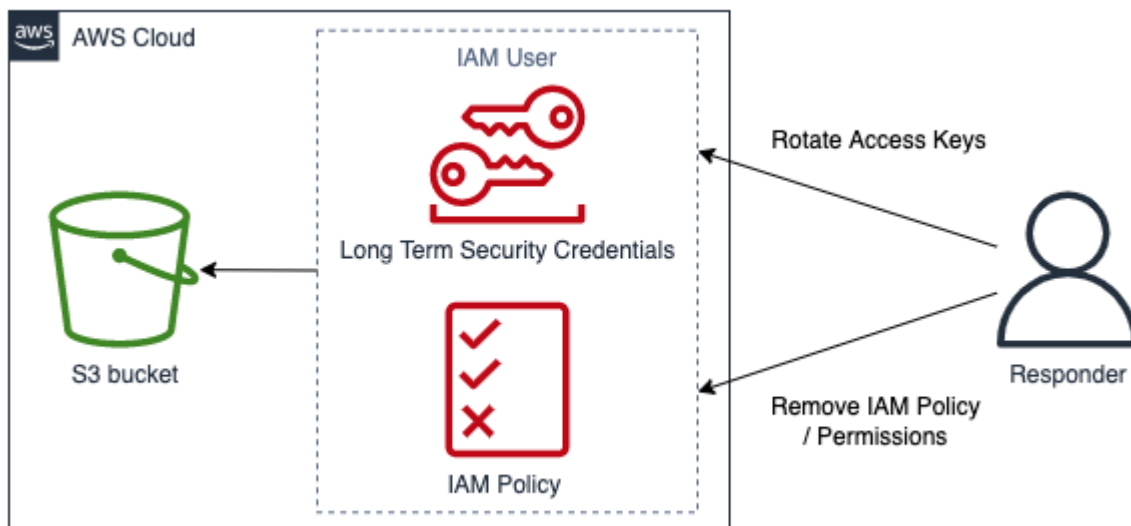
Technik und Eingrenzung des Zugangs

Verhindern Sie die unbefugte Nutzung einer Ressource, indem Sie die Funktionen und IAM Prinzipale einschränken, die Zugriff auf die Ressource haben. Dazu gehört die Einschränkung der Berechtigungen von IAM Prinzipalen, die Zugriff auf die Ressource haben. Dazu gehört auch der vorübergehende Widerruf von Sicherheitsanmeldeinformationen. Beispiele für Technik und Zugriffskontrolle mithilfe von AWS Diensten werden hier hervorgehoben:

- **Berechtigungen einschränken** — Die einem IAM Principal zugewiesenen Berechtigungen sollten dem [Prinzip der geringsten Rechte entsprechen](#). Während eines aktiven Sicherheitsereignisses müssen Sie jedoch möglicherweise den Zugriff auf eine Zielressource von einem bestimmten IAM Prinzipal aus noch weiter einschränken. In diesem Fall ist es möglich, den Zugriff auf eine Ressource einzuschränken, indem dem IAM Prinzipal die entsprechenden Rechte entzogen werden. Dies erfolgt mit dem IAM Dienst und kann mit dem AWS Management Console AWS CLI, dem oder einem angewendet werden AWS SDK.
- **Schlüssel widerrufen** — IAM Zugriffsschlüssel werden von IAM Prinzipalen verwendet, um auf Ressourcen zuzugreifen oder diese zu verwalten. [Dabei handelt es sich um statische Langzeitanmeldedaten, mit denen programmatische Anfragen an AWS CLI oder signiert werden AWS API und mit dem Präfix beginnen AKIA\(weitere Informationen finden Sie im IAM Abschnitt Grundlegendes zu eindeutigen ID-Präfixen unter Identifikatoren\)](#). Um einem IAM Prinzipal Zugriff zu gewähren, wenn ein IAM Zugriffsschlüssel kompromittiert wurde, kann der Zugriffsschlüssel deaktiviert oder gelöscht werden. Es ist wichtig, Folgendes zu beachten:
 - Ein Zugriffsschlüssel kann reaktiviert werden, nachdem er deaktiviert wurde.
 - Ein Zugriffsschlüssel kann nicht wiederhergestellt werden, sobald er gelöscht wurde.
 - Ein IAM Principal kann bis zu zwei Zugriffsschlüssel gleichzeitig haben.
 - Benutzer oder Anwendungen, die den Zugriffsschlüssel verwenden, verlieren den Zugriff, sobald der Schlüssel entweder deaktiviert oder gelöscht wird.
- **Temporäre Sicherheitsanmeldedaten widerrufen** — Temporäre Sicherheitsanmeldedaten können von einer Organisation verwendet werden, um den Zugriff auf AWS Ressourcen zu kontrollieren. Beginnen Sie mit dem Präfix ASIA(weitere Informationen finden Sie im Abschnitt Grundlegendes zu eindeutigen ID-Präfixen unter [IAMIdentifikatoren](#)). Temporäre Anmeldeinformationen werden in der Regel von IAM Rollen verwendet und müssen nicht rotiert oder explizit gesperrt werden, da sie eine begrenzte Gültigkeitsdauer haben. In Fällen, in denen vor Ablauf der temporären Anmeldeinformationen ein Sicherheitsereignis eintritt, müssen Sie möglicherweise die effektiven Berechtigungen der vorhandenen temporären Anmeldeinformationen ändern. Dies kann [mithilfe des darin enthaltenen IAM Dienstes](#) abgeschlossen werden. AWS Management Console Temporäre Sicherheitsanmeldedaten können auch IAM Benutzern (im Gegensatz zu IAM Rollen) ausgestellt werden. Zum Zeitpunkt der Erstellung dieses Artikels gibt es jedoch keine Möglichkeit, die temporären Sicherheitsanmeldedaten für einen IAM Benutzer innerhalb von zu widerrufen AWS Management Console. Bei Sicherheitsereignissen, bei denen der IAM Zugriffsschlüssel eines Benutzers durch einen nicht autorisierten Benutzer kompromittiert wird, der temporäre Sicherheitsanmeldeinformationen erstellt hat, können die temporären Sicherheitsanmeldedaten auf zwei Arten gesperrt werden:

- Fügen Sie dem IAM Benutzer eine Inline-Richtlinie hinzu, die den Zugriff auf die Dauer der Ausgabe des Sicherheitstokens verhindert (weitere Informationen finden Sie im Abschnitt Sperren des Zugriffs auf temporäre Sicherheitsanmeldeinformationen, die vor einem bestimmten Zeitpunkt ausgestellt wurden, unter [Berechtigungen für temporäre Sicherheitsanmeldeinformationen deaktivieren](#)).
- Löschen Sie den IAM Benutzer, dem die kompromittierten Zugriffsschlüssel gehören. Erstellen Sie den Benutzer bei Bedarf erneut.
- AWS WAF- Bestimmte Techniken, die von nicht autorisierten Benutzern eingesetzt werden, beinhalten häufig auftretende böswillige Datenverkehrsmuster, wie Anfragen, die SQL Injection und Cross-Site Scripting beinhalten (). XSS AWS WAF kann mithilfe der AWS WAF integrierten Regelanweisungen so konfiguriert werden, dass der Datenverkehr mithilfe dieser Techniken abgeblockt und abgewiesen wird.

Ein Beispiel für Technik und Zugriffskontrolle finden Sie in der folgenden Abbildung. Ein Incident-Responder rotiert die Zugriffsschlüssel oder entfernt eine IAM Richtlinie, um zu verhindern, dass ein IAM Benutzer auf einen Amazon S3 S3-Bucket zugreift.



Beispiel für Technik und Zugangskontrolle

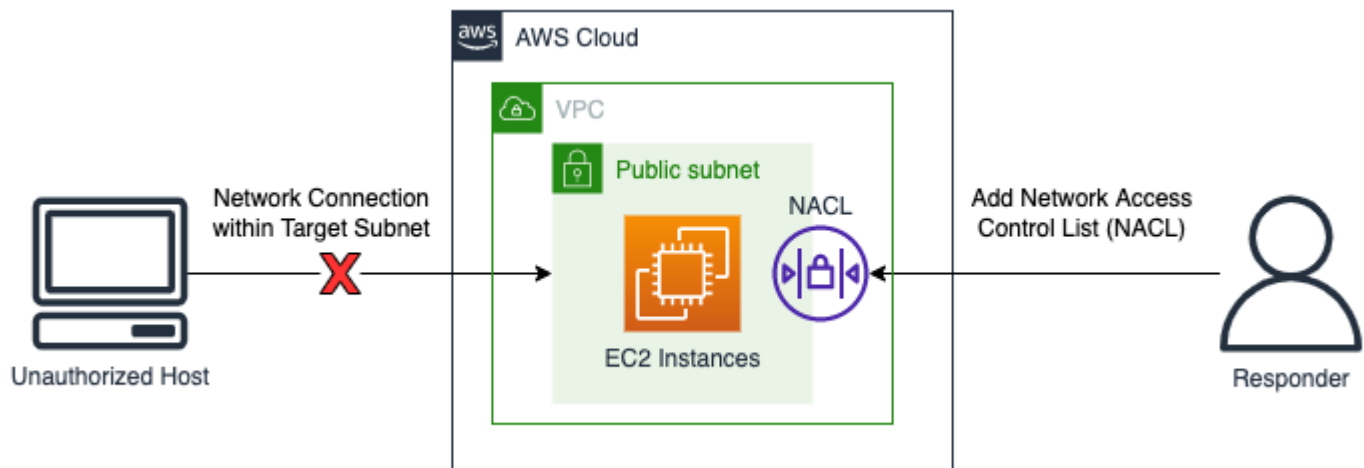
Eindämmung des Ziels

Unter Destination Containment versteht man die Anwendung von Filterung oder Routing innerhalb einer Umgebung, um den Zugriff auf einen Zielhost oder eine Zielressource zu verhindern. In einigen Fällen beinhaltet die Eindämmung von Zielen auch eine Form der Resilienz, um zu überprüfen, ob legitime Ressourcen repliziert werden, um ihre Verfügbarkeit sicherzustellen. Ressourcen sollten aus

Gründen der Isolierung und Eindämmung von diesen Formen der Resilienz getrennt werden. Zu den Beispielen für die Eindämmung von Zielen mithilfe von Diensten gehören: AWS

- **Netzwerk ACLs** — Für Netzwerke ACLs (NetzwerkeACLs), die in Subnetzen konfiguriert sind, die AWS Ressourcen enthalten, können Ablehnungsregeln hinzugefügt werden. Diese Ablehnungsregeln können angewendet werden, um den Zugriff auf eine bestimmte AWS Ressource zu verhindern. Die Anwendung der Netzwerkzugriffskontrollliste (NetzwerkACL) wirkt sich jedoch auf alle Ressourcen im Subnetz aus, nicht nur auf die Ressourcen, auf die unautorisiert zugegriffen wird. Die in einem Netzwerk aufgelisteten Regeln ACL werden von oben nach unten verarbeitet. Daher ACL sollte die erste Regel in einem vorhandenen Netzwerk so konfiguriert werden, dass nicht autorisierter Datenverkehr zur Zielressource und zum Zielsubnetz verweigert wird. Alternativ ACL kann ein völlig neues Netzwerk mit einer einzigen Ablehnungsregel für eingehenden und ausgehenden Verkehr erstellt und dem Subnetz zugeordnet werden, das die Zielressource enthält, um den Zugriff auf das Subnetz über das neue Netzwerk zu verhindern. ACL
- **Herunterfahren** — Das vollständige Herunterfahren einer Ressource kann wirksam sein, um die Auswirkungen einer unbefugten Nutzung einzudämmen. Das Herunterfahren einer Ressource verhindert auch den legitimen Zugriff für geschäftliche Zwecke und verhindert, dass flüchtige forensische Daten abgerufen werden. Daher sollte dies eine gezielte Entscheidung sein und anhand der Sicherheitsrichtlinien eines Unternehmens beurteilt werden.
- **Isolierung VPCs** — Die Isolierung VPCs kann verwendet werden, um Ressourcen effektiv einzudämmen und gleichzeitig Zugriff auf legitimen Datenverkehr zu gewähren (z. B. Antiviren- (AV) oder EDR Lösungen, die Zugriff auf das Internet oder eine externe Managementkonsole erfordern). Die Isolierung VPCs kann vor einem Sicherheitsereignis so vorkonfiguriert werden, dass gültige IP-Adressen und Ports zugelassen werden. VPC Während eines aktiven Sicherheitsereignisses können gezielte Ressourcen sofort in diese Isolierung verschoben werden, um die Ressource einzudämmen und gleichzeitig zu ermöglichen, dass legitimer Datenverkehr von der Zielressource in nachfolgenden Phasen der Reaktion auf Vorfälle gesendet und empfangen werden kann. Ein wichtiger Aspekt der Verwendung einer Isolierung VPC besteht darin, dass Ressourcen, wie z. B. EC2 Instanzen, VPC vor der Verwendung heruntergefahren und in der neuen Isolierung neu gestartet werden müssen. Bestehende EC2 Instanzen können nicht in eine andere VPC oder eine andere Availability Zone verschoben werden. Folgen Sie dazu den Schritten unter [Wie verschiebe ich meine EC2 Amazon-Instance in ein anderes Subnetz, in eine Availability Zone oder VPC?](#)
- **Auto Scaling Scaling-Gruppen und Load Balancer** — AWS Ressourcen, die Auto Scaling Scaling-Gruppen und Load Balancers zugeordnet sind, sollten im Rahmen der Zieleindämmungsverfahren getrennt und deregistriert werden. Das Trennen und Deregistrieren von AWS Ressourcen kann mit dem, und durchgeführt werden. AWS Management Console AWS CLI AWS SDK

Das folgende Diagramm zeigt ein Beispiel für die Eindämmung von Zielen. Ein Incident Response Analyst fügt einem Subnetz ein Netzwerk hinzuACL, um eine Netzwerkverbindungsanfrage von einem nicht autorisierten Host zu blockieren.



Beispiel für die Eindämmung eines Ziels

Übersicht

Die Eindämmung ist ein Schritt der Reaktion auf Vorfälle und kann manuell oder automatisiert erfolgen. Die allgemeine Eindämmungsstrategie sollte sich an den Sicherheitsrichtlinien und Geschäftsanforderungen eines Unternehmens orientieren und sicherstellen, dass negative Auswirkungen vor der Beseitigung und Wiederherstellung so effizient wie möglich abgemildert werden.

Beseitigung

Bei der Beseitigung von Sicherheitsvorfällen handelt es sich um die Entfernung verdächtiger oder nicht autorisierter Ressourcen, um das Konto wieder in einen bekannten sicheren Zustand zu versetzen. Die Strategie zur Beseitigung hängt von mehreren Faktoren ab, die von den Geschäftsanforderungen Ihres Unternehmens abhängen.

Der [NISTSP 800-61 Leitfaden zur Behandlung von Computersicherheitsvorfällen](#) enthält mehrere Schritte zur Beseitigung von Sicherheitsvorfällen:

1. Identifizieren und beheben Sie alle Sicherheitslücken, die ausgenutzt wurden.
2. Entfernen Sie Malware, unangemessene Materialien und andere Komponenten.

3. Wenn weitere betroffene Hosts entdeckt werden (z. B. neue Malware-Infektionen), wiederholen Sie die Erkennungs- und Analyseschritte, um alle anderen betroffenen Hosts zu identifizieren und den Vorfall dann einzudämmen und zu beseitigen.

Bei AWS Ressourcen kann dies anhand der Ereignisse, die mithilfe verfügbarer Protokolle oder automatisierter Tools wie CloudWatch Logs und Amazon GuardDuty erkannt und analysiert werden, weiter verfeinert werden. Diese Ereignisse sollten als Grundlage für die Entscheidung dienen, welche Abhilfemaßnahmen durchgeführt werden sollten, um die Umgebung ordnungsgemäß wieder in einen bekannten sicheren Zustand zu versetzen.

Im ersten Schritt der Ausrottung wird festgestellt, welche Ressourcen innerhalb des AWS Kontos betroffen sind. Dies wird durch die Analyse Ihrer verfügbaren Protokollquellen und Ressourcen und automatisierter Tools erreicht.

- Identifizieren Sie unbefugte Aktionen, die von den IAM Identitäten in Ihrem Konto ausgeführt wurden.
- Identifizieren Sie unbefugte Zugriffe oder Änderungen an Ihrem Konto.
- Identifizieren Sie die Erstellung nicht autorisierter Ressourcen oder IAM Benutzer.
- Identifizieren Sie Systeme oder Ressourcen mit nicht autorisierten Änderungen.

Sobald die Liste der Ressourcen identifiziert ist, sollten Sie jede einzelne überprüfen, um festzustellen, welche Auswirkungen das Löschen oder Wiederherstellen der Ressource auf Ihr Unternehmen hat. Wenn beispielsweise ein Webserver Ihre Geschäftsanwendung hostet und das Löschen dieser Anwendung zu Ausfallzeiten führen würde, sollten Sie in Betracht ziehen, die Ressource aus verifizierten sicheren Backups wiederherzustellen oder das System von einem sauberen System neu zu starten, AMI bevor Sie den betroffenen Server löschen.

Sobald Sie Ihre Geschäftsauswirkungsanalyse abgeschlossen haben, sollten Sie anhand der Ereignisse aus Ihrer Protokollanalyse die Konten überprüfen und die entsprechenden Abhilfemaßnahmen durchführen, z. B.:

- Schlüssel rotieren oder löschen — durch diesen Schritt wird dem Akteur die Möglichkeit genommen, weiterhin Aktivitäten innerhalb des Accounts auszuführen.
- Potenziell nicht autorisierte IAM Benutzeranmeldedaten rotieren.
- Löschen Sie unbekannte oder nicht autorisierte Ressourcen.

Important

Wenn Sie Ressourcen für Ihre Untersuchung behalten müssen, sollten Sie erwägen, diese Ressourcen zu sichern. Wenn Sie beispielsweise eine EC2 Amazon-Instance aus regulatorischen, behördlichen oder rechtlichen Gründen behalten müssen, [erstellen Sie einen EBS Amazon-Snapshot](#), bevor Sie die Instance entfernen.

- Bei Malware-Infektionen müssen Sie sich möglicherweise an einen AWS Partner oder einen anderen Anbieter wenden. AWS bietet keine systemeigenen Tools für die Analyse oder Entfernung von Malware. Wenn Sie jedoch das GuardDuty Malware-Modul für Amazon verwenden, sind möglicherweise Empfehlungen für die bereitgestellten Ergebnisse verfügbar.

Sobald Sie die identifizierten betroffenen Ressourcen gelöscht haben, AWS empfiehlt Ihnen, eine Sicherheitsüberprüfung Ihres Kontos durchzuführen. Dies kann mithilfe von AWS Config Regeln, mithilfe von Open-Source-Lösungen wie Prowler und/oder durch andere Anbieter ScoutSuite geschehen. Sie sollten auch in Betracht ziehen, Sicherheitslücken in Ihren öffentlich zugänglichen Ressourcen (Internet) zu scannen, um das Restrisiko einzuschätzen.

Die Beseitigung ist ein Schritt der Reaktion auf Vorfälle und kann je nach Vorfall und betroffenen Ressourcen manuell oder automatisiert erfolgen. Die Gesamtstrategie sollte sich an den Sicherheitsrichtlinien und Geschäftsanforderungen eines Unternehmens orientieren und sicherstellen, dass negative Auswirkungen durch das Entfernen ungeeigneter Ressourcen oder Konfigurationen gemildert werden.

Wiederherstellung

Bei der Wiederherstellung werden Systeme in einen bekannten sicheren Zustand zurückversetzt, wobei vor der Wiederherstellung überprüft wird, ob Backups sicher sind oder nicht vom Vorfall betroffen sind. Außerdem werden Tests durchgeführt, um sicherzustellen, dass die Systeme nach der Wiederherstellung ordnungsgemäß funktionieren, und die Behebung von Sicherheitslücken im Zusammenhang mit dem Sicherheitsereignis.

Die Reihenfolge der Wiederherstellung hängt von den Anforderungen Ihres Unternehmens ab. Im Rahmen des Wiederherstellungsprozesses sollten Sie eine Analyse der Geschäftsauswirkungen durchführen, um mindestens Folgendes zu ermitteln:

- Geschäftsprioritäten oder Prioritäten bei Abhängigkeiten
- Der Wiederherstellungsplan

- Authentifizierung und Autorisierung

Der NIST SP 800-61 Computer Security Incident Handling Guide enthält mehrere Schritte zur Wiederherstellung von Systemen, darunter:

- Wiederherstellung von Systemen aus sauberen Backups.
 - Stellen Sie sicher, dass die Backups vor der Wiederherstellung auf den Systemen geprüft wurden, um sicherzustellen, dass die Infektion nicht vorhanden ist, und um ein erneutes Auftreten des Sicherheitsereignisses zu verhindern.

Backups sollten im Rahmen von Disaster-Recovery-Tests regelmäßig überprüft werden, um sicherzustellen, dass der Backup-Mechanismus ordnungsgemäß funktioniert und die Datenintegrität den Wiederherstellungszielen entspricht.

- Verwenden Sie nach Möglichkeit Backups, die vor dem Zeitstempel des ersten Ereignisses erstellt wurden, das im Rahmen der Ursachenanalyse ermittelt wurde.
- Neuaufbau von Systemen von Grund auf, einschließlich der Neubereitstellung aus einer vertrauenswürdigen Quelle mithilfe von Automatisierung, manchmal in einem neuen Konto. AWS
- Kompromittierte Dateien durch saubere Versionen ersetzen.

Sie sollten dabei große Vorsicht walten lassen. Sie müssen absolut sicher sein, dass die Datei, die Sie wiederherstellen, als sicher gilt und von dem Vorfall nicht betroffen ist

- Patches werden installiert.
- Passwörter ändern.
 - Dazu gehören Passwörter für IAM Schulleiter, die möglicherweise missbraucht wurden.
 - Wenn möglich, empfehlen wir die Verwendung von Rollen für IAM Prinzipale und Verbund als Teil einer Strategie der geringsten Rechte.
- Verschärfung der Netzwerkperimetersicherheit (Firewall-Regelsätze, Zugriffskontrolllisten für Boundary-Router).

Sobald die Ressourcen wiederhergestellt sind, ist es wichtig, die gewonnenen Erkenntnisse zu nutzen, um Richtlinien, Verfahren und Leitfäden zur Reaktion auf Vorfälle zu aktualisieren.

Zusammenfassend lässt sich sagen, dass es unerlässlich ist, einen Wiederherstellungsprozess zu implementieren, der die Rückkehr zu bekanntermaßen sicheren Abläufen erleichtert.

Die Wiederherstellung kann lange dauern und erfordert eine enge Verknüpfung mit Eindämmungsstrategien, um die geschäftlichen Auswirkungen gegen das Risiko einer

erneuten Infektion abzuwägen. Die Wiederherstellungsverfahren sollten Schritte zur Wiederherstellung von Ressourcen und Diensten sowie von Kunden und IAM die Durchführung einer Sicherheitsüberprüfung des Kontos zur Bewertung des Restrisikos umfassen.

Schlussfolgerung

Jede Betriebsphase hat eigene Ziele, Techniken, Methoden und Strategien. Tabelle 4 fasst diese Phasen und einige der in diesem Abschnitt behandelten Techniken und Methoden zusammen.

Tabelle 4 — Betriebsphasen: Ziele, Techniken und Methoden

Phase	Ziel	Techniken und Methoden
Erkennung	Identifizieren eines potenziellen Sicherheitsereignisses.	<ul style="list-style-type: none"> • Sicherheitskontrollen zur Erkennung • Verhaltens- und regelbasierte Erkennung • Personengestützte Erkennung
Analyse	Stellen Sie fest, ob es sich bei dem Sicherheitsereignis um einen Vorfall handelt, und beurteilen Sie den Umfang des Vorfalls.	<ul style="list-style-type: none"> • Validierung und Umfang der Warnung • Logs abfragen • Informationen zu Bedrohungen • Automatisierung
Eindämmung	Minimiert und begrenzt die Auswirkungen des Sicherheitsereignisses.	<ul style="list-style-type: none"> • Eingrenzung der Quelle • Technik und Eindämmung des Zugangs • Eindämmung des Ziels
Ausrottung	Entfernen nicht autorisierter Ressourcen oder Artefakte im Zusammenhang mit dem Sicherheitsereignis.	<ul style="list-style-type: none"> • Kompromittierte oder unbefugte Rotation oder Löschung von Anmeldeinformationen

Phase	Ziel	Techniken und Methoden
		<ul style="list-style-type: none"> • Unbefugtes Löschen von Ressourcen • Entfernung von Schadsoftware • Sicherheitsscans
Wiederherstellung	Stellen Sie den zweifelsfrei funktionierenden Zustand der Systeme wieder her und überwachen Sie diese Systeme, um sicherzustellen, dass die Bedrohung nicht erneut auftritt.	<ul style="list-style-type: none"> • Systemwiederherstellung anhand von Backups • Systeme wurden von Grund auf neu aufgebaut • Kompromittierte Dateien wurden durch saubere Versionen ersetzt

Aktivität nach Vorfällen

Die Bedrohungslage ändert sich ständig, und es ist wichtig, dass Ihre Organisation ebenso dynamisch in der Lage ist, Ihre Umgebungen wirksam zu schützen. Der Schlüssel zur kontinuierlichen Verbesserung liegt darin, die Ergebnisse Ihrer Vorfälle und Simulationen immer wieder zu überprüfen, um Ihre Fähigkeiten zur effektiven Erkennung, Reaktion und Untersuchung möglicher Sicherheitsvorfälle zu verbessern und so Ihre möglichen Sicherheitslücken zu reduzieren, die Reaktionszeit zu verkürzen und den sicheren Betrieb wieder aufzunehmen. Mithilfe der folgenden Mechanismen können Sie überprüfen, ob Ihre Organisation über die neuesten Funktionen und Kenntnisse verfügt, um unabhängig von der Situation effektiv reagieren zu können.

Schaffen Sie einen Rahmen, um aus Vorfällen zu lernen

Die Implementierung eines Rahmens und einer Methodik aus den gewonnenen Erkenntnissen wird nicht nur dazu beitragen, die Reaktionsfähigkeit zu verbessern, sondern auch dazu beitragen, zu verhindern, dass sich der Vorfall wiederholt. Indem Sie aus jedem Vorfall lernen, können Sie verhindern, dass sich dieselben Fehler, Risiken oder Fehlkonfigurationen wiederholen. Dies verbessert nicht nur Ihre Sicherheitslage, sondern minimiert auch den Zeitverlust durch vermeidbare Situationen.

Es ist wichtig, ein Erkenntnis-Framework zu implementieren, das ganz allgemein Folgendes ermittelt und erreicht:

- Wann kommt es zu Erkenntnissen?
- Was beinhaltet der Erkenntnisprozess?
- Wie werden Erkenntnisse gewonnen?
- Wer ist auf welche Weise an dem Prozess beteiligt?
- Wie werden verbesserungswürdige Bereiche identifiziert?
- Wie stellen Sie sicher, dass die Verbesserungen effektiv verfolgt und umgesetzt werden?

Abgesehen von den aufgeführten Ergebnissen auf hoher Ebene ist es wichtig, sicherzustellen, dass Sie die richtigen Fragen stellen, um den größtmöglichen Nutzen aus dem Prozess zu ziehen (Informationen, die zu umsetzbaren Verbesserungen führen). Berücksichtigen Sie die folgenden Fragen, um Ihre Diskussionen über Erkenntnisse zu fördern:

- Was ist vorgefallen?
- Wann wurde der Vorfall zum ersten Mal identifiziert?
- Wie wurde er identifiziert?
- Von welchen Systemen wurde eine Warnung im Zusammenhang mit der Aktivität ausgegeben?
- Welche Systeme, Services und Daten waren beteiligt?
- Was ist konkret passiert?
- Was hat gut funktioniert?
- Was hat nicht gut funktioniert?
- Welcher Prozess oder welche Verfahren haben versagt oder konnten nicht skaliert werden, um auf den Vorfall zu reagieren?
- Was kann in den folgenden Bereichen verbessert werden:
 - Personen
 - Waren die Mitarbeiter, die kontaktiert werden mussten, tatsächlich verfügbar und war die Kontaktliste auf dem neuesten Stand?
 - Fehlten den Mitarbeitern Schulungen oder Fähigkeiten, die erforderlich waren, um effektiv auf den Vorfall reagieren und ihn untersuchen zu können?
 - Waren die erforderlichen Ressourcen bereit und verfügbar?
 - Prozess

- Wurden Prozesse und Verfahren eingehalten?
- Waren Prozesse und Verfahren für diesen Vorfall bzw. für diese Art von Vorfall dokumentiert und verfügbar?
- Fehlten erforderliche Prozesse und Verfahren?
- Konnten die Notfallteams rechtzeitig auf die erforderlichen Informationen zugreifen, um auf das Problem zu reagieren?
- Technologie
 - Haben die bestehenden Warnsysteme die Aktivität effektiv identifiziert und gemeldet?
 - Müssen bestehende Warnungen verbessert oder neue Warnungen für diesen Vorfall bzw. für diese Art von Vorfall erstellt werden?
 - Ermöglichen die vorhandenen Tools eine effektive Untersuchung (Suche/Analyse) des Vorfalls?
- Was kann getan werden, um diesen Vorfall bzw. diese Art von Vorfall früher zu erkennen?
- Was kann getan werden, um zu verhindern, dass sich dieser Vorfall bzw. diese Art von Vorfall wiederholt?
- Wer ist für den Verbesserungsplan zuständig und wie testen Sie, ob er implementiert wurde?
- Wie sieht der Zeitplan für die Implementierung und Erprobung der zusätzlichen monitoring/preventative controls/process Maßnahmen aus?

Diese Liste ist nicht vollständig. Sie soll als Ausgangspunkt dienen, um zu ermitteln, welche Anforderungen das Unternehmen und das Unternehmen haben und wie Sie diese analysieren können, um am effektivsten aus Vorfällen zu lernen und Ihre Sicherheitslage kontinuierlich zu verbessern. Am wichtigsten ist, damit zu beginnen und Erkenntnisse standardmäßig in Ihren Prozess zur Vorfallreaktion, in die Dokumentation und in die Erwartungen der Stakeholder zu integrieren.

Legen Sie Erfolgskennzahlen fest

Kennzahlen sind notwendig, um Ihre Fähigkeiten zur Reaktion auf Vorfälle effektiv zu messen, zu bewerten und zu verbessern. Ohne Kennzahlen gibt es keine Referenz, anhand derer Sie genau messen oder sogar identifizieren können, wie gut Ihr Unternehmen abschneidet (oder nicht). Es gibt einige Kennzahlen, die bei der Reaktion auf Vorfälle üblich sind. Sie sind ein guter Ausgangspunkt für ein Unternehmen, das Erwartungen und Referenzen für das Streben nach operativer Exzellenz ermitteln möchte.

Durchschnittliche Zeit bis zur Erkennung

Die durchschnittliche Erkennungszeit ist die durchschnittliche Zeit, die benötigt wird, um einen möglichen Sicherheitsvorfall zu entdecken. Konkret ist dies die Zeit zwischen dem Auftreten des ersten Bedrohungsindikators und der ersten Identifizierung oder Warnung.

Mit dieser Metrik können Sie nachverfolgen, wie effektiv Ihre Erkennungs- und Warnsysteme arbeiten. Effektive Erkennungs- und Warnmechanismen sind entscheidend, um sicherzustellen, dass sich mögliche Sicherheitsvorfälle nicht in Ihren Umgebungen fortsetzen.

Je länger die durchschnittliche Erkennungszeit ist, desto größer ist die Notwendigkeit, zusätzliche oder effektivere Warnmeldungen und Mechanismen zur Identifizierung und Entdeckung möglicher Sicherheitsvorfälle zu entwickeln. Je kürzer die durchschnittliche Erkennungszeit ist, desto besser funktionieren Ihre Erkennungs- und Warnmechanismen.

Durchschnittliche Zeit bis zur Bestätigung

Die durchschnittliche Zeit bis zur Bestätigung ist die durchschnittliche Zeit, die benötigt wird, um einen möglichen Sicherheitsvorfall zu bestätigen und zu priorisieren. Konkret handelt es sich dabei um die Zeit zwischen der Generierung einer Warnung und der Identifizierung und Priorisierung der Warnung durch einen Ihrer Mitarbeiter SOC oder Mitarbeiter zur Reaktion auf Vorfälle.

Anhand dieser Kennzahl können Sie nachverfolgen, wie gut Ihr Team Warnmeldungen bearbeitet und priorisiert. Wenn Ihr Team nicht in der Lage ist, Benachrichtigungen effektiv zu identifizieren und zu priorisieren, werden die Antworten verzögert und sind ineffektiv.

Je länger die durchschnittliche Zeit bis zur Bestätigung ist, desto größer ist die Notwendigkeit, sicherzustellen, dass Ihr Team sowohl über angemessene Ressourcen als auch über Schulungen verfügt, um einen möglichen Sicherheitsvorfall schnell zu erkennen und zu priorisieren, um darauf zu reagieren. Je kürzer die durchschnittliche Zeit bis zur Bestätigung ist, desto besser reagiert Ihr Team auf Sicherheitswarnungen und zeigt, dass es effektiv vorbereitet ist und in der Lage ist, sie gut zu priorisieren.

Durchschnittliche Reaktionszeit

Die durchschnittliche Reaktionszeit ist die durchschnittliche Zeit, die benötigt wird, um mit der ersten Reaktion auf einen möglichen Sicherheitsvorfall zu beginnen. Konkret ist dies die Zeit zwischen der ersten Warnung oder Entdeckung eines möglichen Sicherheitsvorfalls und den ersten Maßnahmen zur Reaktion darauf. Dies entspricht der mittleren Zeit bis zur Bestätigung, ist jedoch die Messung

bestimmter Reaktionsmaßnahmen (z. B. Erfassung von Systemdaten, Eindämmung des Systems) im Vergleich zur einfachen Erkennung oder Bestätigung der Situation.

Anhand dieser Kennzahl können Sie nachverfolgen, wie gut Sie auf Sicherheitsvorfälle vorbereitet sind. Wie bereits erwähnt, ist die Vorbereitung der Schlüssel zu einer effektiven Reaktion. Weitere Informationen finden Sie im [the section called "Vorbereitung"](#) Abschnitt dieses Dokuments.

Je länger die durchschnittliche Reaktionszeit ist, desto größer ist die Notwendigkeit, sicherzustellen, dass Ihr Team in der richtigen Vorgehensweise geschult ist, damit die Reaktionsprozesse effektiv dokumentiert und genutzt werden. Je kürzer die durchschnittliche Reaktionszeit ist, desto besser ist Ihr Team darin, eine angemessene Reaktion auf identifizierte Warnungen zu finden und die erforderlichen Reaktionsmaßnahmen zu ergreifen, um den Weg zurück zu einem sicheren Betrieb zu beginnen.

Durchschnittliche Eindämmungszeit

Die durchschnittliche Zeit bis zur Eindämmung ist die durchschnittliche Zeit, die benötigt wird, um einen möglichen Sicherheitsvorfall einzudämmen. Konkret handelt es sich dabei um die Zeit zwischen der ersten Warnung oder Entdeckung eines möglichen Sicherheitsvorfalls und dem Abschluss von Gegenmaßnahmen, die wirksam verhindern, dass der Angreifer oder die kompromittierten Systeme weiteren Schaden anrichten.

Anhand dieser Kennzahl können Sie nachverfolgen, wie gut Ihr Team in der Lage ist, mögliche Sicherheitsvorfälle einzudämmen oder einzudämmen. Die Unfähigkeit, mögliche Sicherheitsvorfälle schnell und effektiv einzudämmen, erhöht die Auswirkungen, den Umfang und die Gefahr, dass weitere Sicherheitsvorfälle gefährdet werden.

Je länger die durchschnittliche Eindämmungszeit ist, desto größer ist die Notwendigkeit, sowohl Wissen als auch Fähigkeiten aufzubauen, um die bei Ihnen auftretenden Sicherheitsvorfälle schnell und effektiv zu mindern und einzudämmen. Je kürzer die mittlere Eindämmungszeit ist, desto besser versteht Ihr Team die erforderlichen Maßnahmen zur Abwehr und Eindämmung identifizierter Bedrohungen und setzt sie um, um die Auswirkungen, den Umfang und die Risiken für das Unternehmen zu verringern.

Durchschnittliche Erholungszeit

Die durchschnittliche Zeit bis zur Wiederherstellung ist die durchschnittliche Zeit, die benötigt wird, um den Betrieb nach einem möglichen Sicherheitsvorfall wieder vollständig wiederherzustellen. Konkret ist dies die Zeit zwischen der ersten Warnung oder der Entdeckung eines möglichen

Sicherheitsvorfalls und dem Zeitpunkt, zu dem das Unternehmen wieder normal und sicher arbeitet, ohne von dem Vorfall betroffen zu sein.

Anhand dieser Kennzahl können Sie nachverfolgen, wie effektiv Ihre Teams dabei sind, Systeme, Konten und Umgebungen nach einem Sicherheitsvorfall wieder in sicheren Betrieb zu versetzen. Die Unfähigkeit, schnell oder effektiv zu einem sicheren Betrieb zurückzukehren, kann sich nicht nur auf die Sicherheit auswirken, sondern auch die Auswirkungen und Kosten für das Unternehmen und seine Abläufe erhöhen.

Je länger die durchschnittliche Wiederherstellungszeit ist, desto größer ist die Notwendigkeit, Ihre Teams und Umgebungen auf die geeigneten Mechanismen vorzubereiten (z. B. Failover-Prozesse und CI/CD-Pipelines zur sicheren Wiedereinführung sauberer Systeme), um die Auswirkungen von Sicherheitsvorfällen auf den Betrieb und das Unternehmen zu minimieren. Je kürzer die durchschnittliche Wiederherstellungszeit ist, desto effektiver können Ihre Teams die Auswirkungen von Sicherheitsvorfällen auf Ihren Betrieb und Ihr Geschäft minimieren.

Verweildauer des Angreifers

Die Verweildauer eines Angreifers ist die durchschnittliche Zeit, während der ein nicht autorisierter Benutzer Zugriff auf ein System oder eine Umgebung hat. Dies entspricht der durchschnittlichen Zeit bis zur Eindämmung, mit der Ausnahme, dass der Zeitraum mit dem Zeitpunkt beginnt, zu dem der Angreifer zum ersten Mal Zugriff auf das System oder die Umgebungen erlangt hat, was vor der ersten Warnung oder Entdeckung liegen kann.

Mit dieser Metrik können Sie verfolgen, wie gut viele Ihrer Systeme und Mechanismen zusammenarbeiten, um den Zeitaufwand, den Zugriff und die Möglichkeiten zu reduzieren, die ein Angreifer oder eine Bedrohung hat, Ihre Umgebung zu beeinträchtigen. Die Reduzierung der Verweildauer von Angreifern sollte für Ihre Teams und Ihr Unternehmen oberste Priorität haben.

Je länger die Verweildauer der Angreifer ist, desto wichtiger ist es, herauszufinden, welche Teile des Incident-Response-Prozesses verbessert werden müssen, um sicherzustellen, dass Ihre Teams in der Lage sind, die Auswirkungen und das Ausmaß von Bedrohungen oder Angriffen in Ihren Umgebungen zu minimieren. Je kürzer die Verweildauer der Angreifer ist, desto besser können Ihre Teams die Zeit und die Chancen minimieren, die eine Bedrohung oder ein Angreifer in Ihren Umgebungen hat, wodurch letztlich das Risiko und die Auswirkungen auf Ihren Betrieb und Ihr Geschäft reduziert werden.

Zusammenfassung der Kennzahlen

Durch die Festlegung und Nachverfolgung von Kennzahlen für die Reaktion auf Vorfälle können Sie Ihre Fähigkeiten zur Reaktion auf Vorfälle effektiv messen, bewerten und verbessern. Um dies zu erreichen, gibt es eine Reihe gängiger Kennzahlen zur Reaktion auf Vorfälle, die in diesem Abschnitt hervorgehoben wurden. In Tabelle 5 sind diese Kennzahlen zusammengefasst.

Tabelle 5 — Kennzahlen zur Reaktion auf Vorfälle

Metrik	Beschreibung
Durchschnittliche Erkennungszeit	Durchschnittliche Zeit, die zur Entdeckung eines möglichen Sicherheitsvorfalls benötigt wird
Durchschnittliche Zeit bis zur Bestätigung	Durchschnittliche Zeit, die benötigt wird, um einen möglichen Sicherheitsvorfall zu bestätigen (und zu priorisieren)
Durchschnittliche Reaktionszeit	Durchschnittliche Zeit, die benötigt wird, um mit der ersten Reaktion auf einen möglichen Sicherheitsvorfall zu beginnen
Durchschnittliche Zeit bis zur Eindämmung	Durchschnittliche Zeit, die benötigt wird, um einen möglichen Sicherheitsvorfall einzudämmen
Durchschnittliche Zeit bis zur Wiederherstellung	Durchschnittliche Zeit bis zur vollständigen Wiederherstellung des Betriebs nach einem möglichen Sicherheitsvorfall
Verweildauer des Angreifers	Durchschnittliche Zeit, in der ein Angreifer Zugriff auf ein System oder eine Umgebung hat

Verwenden Sie Kompromissindikatoren (IOCs)

Ein Indikator für eine Gefährdung (IOC) ist ein Artefakt, das in oder auf einem Netzwerk, System oder einer Umgebung beobachtet wird und das (mit einem hohen Maß an Sicherheit) böswillige Aktivitäten oder einen Sicherheitsvorfall identifizieren kann. IOCskann in einer Vielzahl von Formen vorkommen,

darunter IP-Adressen, Domänen, Artefakte auf Netzwerkebene wie TCP Flags oder Payloads, Artefakte auf System- oder Host-Ebene wie ausführbare Dateien, Dateinamen und Hashes, Protokolldateieinträge oder Registrierungseinträge und mehr. Sie können auch eine Kombination von Elementen oder Aktivitäten sein, z. B. das Vorhandensein bestimmter Elemente oder Artefakte auf einem System (eine bestimmte Datei oder Gruppe von Dateien und Registrierungselementen), Aktionen, die in einer bestimmten Reihenfolge ausgeführt werden (eine Anmeldung bei einem System von einer bestimmten IP aus, gefolgt von bestimmten anomalen Befehlen) oder Netzwerkaktivität (anomalier eingehender oder ausgehender Verkehr zu oder von bestimmten Domänen), die auf eine bestimmte Bedrohungs-, Angriffs- oder Angriffsmethode hinweisen können.

Während Sie daran arbeiten, Ihr Incident-Response-Programm schrittweise zu verbessern, sollten Sie ein Framework zur Erfassung, Verwaltung und Nutzung IOCs als Mechanismus implementieren, um Erkennungen und Warnmeldungen kontinuierlich aufzubauen und zu verbessern und die Geschwindigkeit und Effizienz von Untersuchungen zu verbessern. Sie können damit beginnen, die Erfassung und Verwaltung von Daten IOCs in die Analyse- und Untersuchungsphasen Ihrer Prozesse zur Reaktion auf Vorfälle zu integrieren. Durch proaktives Identifizieren, Sammeln und Speichern IOCs als Standardbestandteil Ihres Prozesses können Sie ein Datenarchiv (als Teil eines umfassenderen Threat-Intelligence-Programms) aufbauen, das wiederum verwendet werden kann, um bestehende Erkennungen und Warnungen zu verbessern, zusätzliche Erkennungen und Warnungen zu erstellen, zu ermitteln, wo und wann ein Artefakt zuvor entdeckt wurde, und Dokumentationen darüber zu erstellen und zu referenzieren, wie Untersuchungen zuvor durchgeführt wurden IOCs, einschließlich Abgleich und mehr.

Kontinuierliche Aus- und Weiterbildung

Allgemeine und berufliche Bildung sind sowohl sich weiterentwickelnde als auch kontinuierliche Anstrengungen, die zielgerichtet fortgeführt und fortgeführt werden sollten. Es gibt eine Vielzahl von Mechanismen, mit denen überprüft werden kann, ob Ihr Team das Bewusstsein, das Wissen und die Fähigkeiten bewahrt, die dem sich entwickelnden Stand der Technik und der Bedrohungslandschaft angemessen sind.

Ein Mechanismus besteht darin, Weiterbildung als Standardbestandteil der Ziele und Abläufe Ihrer Teams einzusetzen. Wie im Abschnitt Vorbereitung erwähnt, müssen Ihre Mitarbeiter und Beteiligten bei der Reaktion auf Vorfälle effektiv darin geschult werden, interne AWS Vorfälle zu erkennen, darauf zu reagieren und zu untersuchen. Bildung ist jedoch kein einmaliges Unterfangen. Die Schulung muss kontinuierlich fortgesetzt werden, um sicherzustellen, dass Ihr Team stets über die neuesten technologischen Fortschritte, Aktualisierungen und Verbesserungen informiert ist, die zur Verbesserung der Wirksamkeit und Effizienz der Reaktion genutzt werden können, sowie über

Ergänzungen oder Aktualisierungen von Daten, die zur Verbesserung von Untersuchungen und Analysen genutzt werden können.

Ein weiterer Mechanismus besteht darin, zu überprüfen, ob Simulationen regelmäßig (z. B. vierteljährlich) durchgeführt werden und sich auf spezifische Ergebnisse für das Unternehmen konzentrieren. Weitere Informationen finden Sie im [the section called “Führen Sie regelmäßige Simulationen durch”](#) Abschnitt dieses Dokuments.

Die Durchführung von ersten Übungen am Tisch ist zwar eine hervorragende Möglichkeit, eine erste Grundlage für Verbesserungen zu schaffen, aber kontinuierliche Tests sind der Schlüssel zu nachhaltigen Verbesserungen und zur Aufrechterhaltung eines up-to-date genauen Abbilds des aktuellen Betriebszustands. Testen Sie anhand der neuesten und kritischsten Sicherheitssituationen und der wichtigsten oder neuesten Reaktionsmöglichkeiten und lassen Sie die gewonnenen Erkenntnisse in die Ausbildung, den Betrieb und die Prozesse/Verfahren einfließen, um sicherzustellen, dass Sie in der Lage sind, Ihre Reaktionsprozesse und Ihr Programm insgesamt kontinuierlich zu verbessern.

Schlussfolgerung

Wenn Sie Ihre Reise in die Cloud fortsetzen, ist es wichtig, dass Sie die grundlegenden Konzepte zur Reaktion auf Sicherheitsvorfälle für Ihre Umgebung berücksichtigen. AWS Sie können die verfügbaren Kontrollen, Cloud-Funktionen und Behebungsoptionen kombinieren, um die Sicherheit Ihrer Cloud-Umgebung zu verbessern. Sie können auch klein anfangen und schrittweise Automatisierungsfunktionen einführen, die Ihre Reaktionsgeschwindigkeit verbessern, sodass Sie besser auf Sicherheitsereignisse vorbereitet sind.

Mitwirkende

Zu den aktuellen und früheren Mitwirkenden an diesem Dokument gehören:

- Anna McAbee, leitende Architektin für Sicherheitslösungen, Amazon Web Services
- Freddy Kasprzykowski, leitender Sicherheitsberater, Amazon Web Services
- Jason Hurst, leitender Sicherheitsingenieur, Amazon Web Services
- Jonathon Poling, Hauptsicherheitsberater, Amazon Web Services
- Josh Du Lac, Senior Manager, Sicherheitslösungsarchitektur, Amazon Web Services
- Paco Hope, leitender Sicherheitsingenieur, Amazon Web Services

- Ryan Tick, leitender Sicherheitsingenieur, Amazon Web Services
- Steve de Vera, leitender Sicherheitsingenieur, Amazon Web Services

Anhang A: Definitionen der Cloud-Funktionen

AWS bietet über 200 Cloud-Dienste und Tausende von Funktionen. Viele von ihnen bieten native Erkennungs-, Präventions- und Reaktionsfunktionen, und andere können zur Entwicklung maßgeschneiderter Sicherheitslösungen verwendet werden. Dieser Abschnitt enthält eine Untergruppe der Dienste, die für die Reaktion auf Vorfälle in der Cloud am relevantesten sind.

Themen

- [Protokollierung und Ereignisse](#)
- [Sichtbarkeit und Alarmierung](#)
- [-Automatisierung](#)
- [Sicherer Speicher](#)
- [Künftige und maßgeschneiderte Sicherheitsfunktionen](#)

Protokollierung und Ereignisse

[AWS CloudTrail](#)— AWS CloudTrail Service, der die Unternehmensführung, die Einhaltung von Vorschriften, die betriebliche Prüfung und die Risikoprüfung von AWS Konten ermöglicht. Mit CloudTrail können Sie Kontoaktivitäten im Zusammenhang mit Aktionen AWS dienstübergreifend protokollieren, kontinuierlich überwachen und speichern. CloudTrail bietet einen Ereignisverlauf Ihrer AWS Kontoaktivitäten, einschließlich Aktionen, die über die AWS Management Console Befehlszeilentools, und andere AWS Dienste ausgeführt wurden. AWS SDKs Dieser Ereignisverlauf vereinfacht die Sicherheitsanalyse, die Nachverfolgung von Ressourcenänderungen und die Fehlerbehebung. CloudTrail protokolliert zwei verschiedene Arten von AWS API Aktionen:

- CloudTrail Verwaltungsereignisse (auch bekannt als Operationen auf der Kontrollebene) zeigen Verwaltungsvorgänge, die mit Ressourcen in Ihrem AWS Konto ausgeführt werden. Dazu gehören Aktionen wie das Erstellen eines Amazon S3 S3-Buckets und das Einrichten der Protokollierung.
- CloudTrail Datenereignisse (auch bekannt als Datenebenenoperationen) zeigen die Ressourcenoperationen, die auf oder innerhalb einer Ressource in Ihrem AWS Konto ausgeführt wurden. Bei diesen Vorgängen handelt es sich häufig um umfangreiche Aktivitäten. Dazu gehören Aktionen wie Amazon S3 API S3-Aktivitäten auf Objektebene (z. B., `GetObjectDeleteObject`, und `PutObject` API Operationen) und Lambda-Funktionsaufrufaktivitäten.

[AWS Config](#)— AWS Config ist ein Service, mit dem Kunden die Konfigurationen Ihrer Ressourcen bewerten, prüfen und bewerten können. AWS Config überwacht und zeichnet Ihre AWS Ressourcenkonfigurationen kontinuierlich auf und ermöglicht es Ihnen, die Auswertung der aufgezeichneten Konfigurationen anhand der gewünschten Konfigurationen zu automatisieren. Mit AWS Config dieser Funktion können Kunden manuell oder automatisch Änderungen an Konfigurationen und Beziehungen zwischen AWS Ressourcen überprüfen, den Verlauf der Ressourcenkonfiguration detailliert nachverfolgen und die allgemeine Konformität mit den in den Kundenrichtlinien angegebenen Konfigurationen ermitteln. Dies ermöglicht eine Vereinfachung von Compliance-Prüfungen, Sicherheitsanalysen, Änderungsmanagement und betrieblicher Fehlerbehebung.

[Amazon EventBridge](#) — Amazon EventBridge liefert nahezu in Echtzeit einen Stream von Systemereignissen, in denen Änderungen bei AWS Ressourcen oder bei der Veröffentlichung von API Aufrufen beschrieben werden. Mithilfe einfacher Regeln, die Sie schnell einrichten können, können Sie Ereignisse zuordnen und sie an eine oder mehrere Zielfunktionen oder Streams weiterleiten. EventBridge wird sich betrieblicher Änderungen bewusst, sobald sie auftreten. EventBridge kann auf diese betrieblichen Änderungen reagieren und bei Bedarf Korrekturmaßnahmen ergreifen, indem es Nachrichten sendet, um auf die Umgebung zu reagieren, Funktionen aktiviert, Änderungen vornimmt und Statusinformationen erfasst. Einige Sicherheitsdienste, wie Amazon GuardDuty, produzieren ihre Ergebnisse in Form von EventBridge Ereignissen. Viele Sicherheitsdienste bieten auch die Möglichkeit, ihre Ausgaben an Amazon S3 zu senden.

Amazon S3 S3-Zugriffsprotokolle — Wenn vertrauliche Informationen in einem Amazon S3 S3-Bucket gespeichert sind, können Kunden Amazon S3 S3-Zugriffsprotokolle aktivieren, um jeden Upload, Download und jede Änderung dieser Daten aufzuzeichnen. Dieses Protokoll ist unabhängig von den CloudTrail Protokollen, die Änderungen am Bucket selbst aufzeichnen (z. B. geänderte Zugriffs- und Lebenszyklusrichtlinien), und zusätzlich zu diesen Protokollen. Es sei darauf hingewiesen, dass die Aufzeichnungen der Zugriffsprotokolle nach bestem Wissen und Gewissen übermittelt werden. Die meisten Anforderungen nach einem Bucket, der für die Protokollierung richtig konfiguriert ist, führen zu einem ausgelieferten Protokollsatz. Die Vollständigkeit und Aktualität der Serverprotokollierung wird nicht garantiert.

[Amazon CloudWatch Logs](#) — Kunden können Amazon CloudWatch Logs verwenden, um Protokolldateien zu überwachen, zu speichern und darauf zuzugreifen, die von Betriebssystemen, Anwendungen und anderen Quellen stammen, die in EC2 Amazon-Instances mit einem CloudWatch Logs-Agenten ausgeführt werden. CloudWatch Protokolle können ein Ziel für Route DNS 53-

Abfragen AWS CloudTrail, VPC Flow-Logs, Lambda-Funktionen und andere sein. Kunden können dann die zugehörigen Protokolldaten aus CloudWatch Logs abrufen.

[Amazon VPC Flow Logs](#) — VPC Flow Logs ermöglicht es Kunden, Informationen über den IP-Verkehr zu und von Netzwerkschnittstellen in zu erfassen VPCs. Nach der Aktivierung von Flow-Logs können sie zu Amazon CloudWatch Logs und Amazon S3 gestreamt werden. VPC Flow Logs unterstützt Kunden bei einer Reihe von Aufgaben, z. B. bei der Behebung von Problemen, warum bestimmter Datenverkehr eine Instance nicht erreicht, bei der Diagnose zu restriktiver Sicherheitsgruppenregeln und bei der Verwendung von Flow Logs als Sicherheitstool zur Überwachung des Datenverkehrs zu EC2 Instances. Verwenden Sie die aktuelle Version der VPC Flow-Protokollierung, um die robustesten Felder zu erhalten.

[AWS WAF Logs](#) — AWS WAF unterstützt die vollständige Protokollierung aller vom Service überprüften Webanfragen. Kunden können diese in Amazon S3 speichern, um Compliance- und Prüfanforderungen sowie Debugging und Forensik zu erfüllen. Diese Protokolle helfen Kunden dabei, die Hauptursache für initiierte Regeln und blockierte Webanfragen zu ermitteln. Protokolle können in Tools von Drittanbietern SIEM und Protokollanalyse-Tools integriert werden.

[Route 53 Resolver-Abfrageprotokolle](#) — Mit Route 53 Resolver-Abfrageprotokollen können Sie alle DNS Abfragen protokollieren, die von Ressourcen innerhalb von Amazon Virtual Private Cloud (AmazonVPC) gestellt wurden. Ganz gleich, ob es sich um eine EC2 Amazon-Instance, eine AWS Lambda Funktion oder einen Container handelt: Wenn es sich in Ihrem Amazon befindet VPC und eine DNS Anfrage stellt, protokolliert diese Funktion diese. Sie können dann untersuchen und besser verstehen, wie Ihre Anwendungen funktionieren.

Andere AWS Protokolle — veröffentlicht AWS kontinuierlich Servicefunktionen und Funktionen für Kunden mit neuen Protokollierungs- und Überwachungsfunktionen. Informationen zu den für die einzelnen AWS Dienste verfügbaren Funktionen finden Sie in unserer öffentlichen Dokumentation.

Sichtbarkeit und Alarmierung

[AWS Security Hub](#) — AWS Security Hub bietet Kunden einen umfassenden Überblick über Sicherheitswarnungen mit hoher Priorität und den kontoübergreifenden Compliance-Status. AWS Security Hub aggregiert, organisiert und priorisiert Ergebnisse von AWS Diensten wie Amazon GuardDuty, Amazon Inspector, Amazon Macie und Lösungen. AWS Partner Die Ergebnisse werden auf integrierten Dashboards mit verwertbaren Grafiken und Tabellen visuell zusammengefasst. Sie können Ihre Umgebung auch kontinuierlich überwachen, indem Sie automatisierte Konformitätsprüfungen verwenden, die auf den AWS bewährten Verfahren und Industriestandards basieren, die Ihr Unternehmen befolgt.

[Amazon GuardDuty](#) — [Amazon GuardDuty](#) ist ein verwalteter Service zur Bedrohungserkennung, der kontinuierlich böses oder unbefugtes Verhalten überwacht, um Kunden beim Schutz von AWS Konten und Workloads zu unterstützen. Es überwacht Aktivitäten wie ungewöhnliche API Aufrufe oder potenziell nicht autorisierte Bereitstellungen, was auf eine mögliche Konto- oder Ressourcenkompromittierung von EC2 Amazon-Instances, Amazon S3-Buckets oder Aufklärungen durch böswillige Akteure hindeutet.

GuardDuty identifiziert mutmaßliche böswillige Akteure mithilfe integrierter Bedrohungsinformationen und nutzt maschinelles Lernen, um Anomalien bei der Konto- und Workload-Aktivität zu erkennen. Wenn eine potenzielle Bedrohung erkannt wird, sendet der Service eine detaillierte Sicherheitswarnung an die GuardDuty Konsole und CloudWatch an Ereignisse. Dadurch sind Warnmeldungen umsetzbar und lassen sich einfach in bestehende Eventmanagement- und Workflow-Systeme integrieren.

GuardDuty bietet außerdem zwei Add-Ons zur Überwachung auf Bedrohungen mit bestimmten Diensten: Amazon GuardDuty für Amazon S3 S3-Schutz und Amazon GuardDuty für EKS Amazon-Schutz. Der Amazon S3 S3-Schutz ermöglicht GuardDuty die Überwachung von API Vorgängen auf Objektebene, um potenzielle Sicherheitsrisiken für Daten in Amazon S3 S3-Buckets zu identifizieren. Der Kubernetes-Schutz ermöglicht GuardDuty die Erkennung verdächtiger Aktivitäten und potenzieller Beeinträchtigungen von Kubernetes-Clustern innerhalb von Amazon. EKS

[Amazon Macie](#) — Amazon Macie ist ein KI-gestützter Sicherheitsservice, der Datenverlust verhindert, indem er sensible Daten, die in gespeichert sind, automatisch erkennt, klassifiziert und schützt. AWS Macie verwendet maschinelles Lernen (ML), um sensible Daten wie personenbezogene Daten (PII) oder geistiges Eigentum zu erkennen, ihnen einen Geschäftswert zuzuweisen und Transparenz darüber zu bieten, wo diese Daten gespeichert sind und wie sie in Ihrem Unternehmen verwendet werden. Amazon Macie überwacht kontinuierlich die Datenzugriffsaktivitäten auf Anomalien und sendet Warnmeldungen, wenn das Risiko eines unbefugten Zugriffs oder unbeabsichtigter Datenlecks erkannt wird.

[AWS-Config-Regeln](#)— Eine AWS Config Regel stellt die bevorzugten Konfigurationen für eine Ressource dar und wird anhand von Konfigurationsänderungen an den entsprechenden Ressourcen bewertet, wie sie von aufgezeichnet wurden. AWS Config Sie können die Ergebnisse der Auswertung einer Regel anhand der Konfiguration einer Ressource in einem Dashboard sehen. Mithilfe von AWS Config Regeln können Sie Ihren allgemeinen Konformitäts- und Risikostatus aus Sicht der Konfiguration beurteilen, Konformitätstrends im Zeitverlauf anzeigen und herausfinden, welche Konfigurationsänderung dazu geführt hat, dass eine Ressource nicht mit einer Regel konform war.

[AWS Trusted Advisor](#)— AWS Trusted Advisor ist eine Online-Ressource, die Ihnen hilft, durch die Optimierung Ihrer AWS Umgebung Kosten zu senken, die Leistung zu steigern und die Sicherheit zu verbessern. Trusted Advisor bietet Anleitungen in Echtzeit, um Sie bei der Bereitstellung Ihrer Ressourcen zu unterstützen und dabei AWS bewährte Methoden zu befolgen. Alle Trusted Advisor Prüfungen, einschließlich der Integration von CloudWatch Ereignissen, stehen Kunden mit Business- und Enterprise Support-Plänen zur Verfügung.

[Amazon CloudWatch](#) — Amazon CloudWatch ist ein Monitoring-Service für AWS Cloud Ressourcen und Anwendungen, auf denen Sie laufen AWS. Sie können CloudWatch damit Kennzahlen sammeln und verfolgen, Protokolldateien sammeln und überwachen, Alarmer einrichten und automatisch auf Änderungen Ihrer AWS Ressourcen reagieren. CloudWatch kann AWS Ressourcen wie EC2 Amazon-Instances, Amazon DynamoDB-Tabellen und Amazon RDS DB-Instances sowie benutzerdefinierte Metriken, die von Ihren Anwendungen und Diensten generiert werden, und alle Protokolldateien, die Ihre Anwendungen generieren, überwachen. Sie können Amazon verwenden CloudWatch , um einen systemweiten Einblick in die Ressourcennutzung, die Anwendungsleistung und den Betriebszustand zu erhalten. Sie können diese Erkenntnisse nutzen, um entsprechend zu reagieren und dafür zu sorgen, dass Ihre Anwendung reibungslos läuft.

[Amazon Inspector](#) — Amazon Inspector ist ein automatisierter Sicherheitsbewertungsservice, der dazu beiträgt, die Sicherheit und Konformität von Anwendungen zu verbessern, auf denen bereitgestellt wird AWS. Amazon Inspector bewertet automatisch Schwachstellen in Anwendungen sowie Abweichungen von bewährten Methoden. Nach der Durchführung einer Bewertung erstellt Amazon Inspector eine detaillierte Liste der Sicherheitsfeststellungen, die nach Schweregrad priorisiert sind. Diese Ergebnisse können direkt oder als Teil detaillierter Bewertungsberichte überprüft werden, die über die Amazon Inspector Inspector-Konsole oder verfügbar sindAPI.

[Amazon Detective](#) — Amazon Detective ist ein Sicherheitsservice, der automatisch Protokolldaten aus Ihren AWS Ressourcen sammelt und mithilfe von maschinellem Lernen, statistischer Analyse und Graphentheorie einen verknüpften Datensatz erstellt, mit dem Sie schnellere und effizientere Sicherheitsuntersuchungen durchführen können. Detective kann Billionen von Ereignissen aus mehreren Datenquellen wie VPC Flow Logs analysieren und GuardDuty erstellt automatisch eine einheitliche, interaktive Ansicht Ihrer Ressourcen, Benutzer und der Interaktionen zwischen ihnen im Laufe der Zeit. CloudTrail Mit dieser einheitlichen Ansicht können Sie alle Details und den Kontext an einem Ort visualisieren, um die zugrunde liegenden Gründe für die Ergebnisse zu ermitteln, relevante historische Aktivitäten zu untersuchen und schnell die Ursache zu ermitteln.

-Automatisierung

[AWS Lambda](#)— AWS Lambda ist ein serverloser Rechendienst, der Ihren Code als Reaktion auf Ereignisse ausführt und die zugrunde liegenden Rechenressourcen automatisch für Sie verwaltet. Sie können Lambda verwenden, um andere AWS Dienste mit benutzerdefinierter Logik zu erweitern, oder Ihre eigenen Backend-Services erstellen, die AWS skalierbar, leistungsstark und sicher arbeiten. Lambda führt Ihren Code auf einer hochverfügbaren Recheninfrastruktur aus und führt die Verwaltung der Rechenressourcen für Sie durch. Dazu gehören Server- und Betriebssystemwartung, Kapazitätsbereitstellung und automatische Skalierung, Bereitstellung von Code- und Sicherheitspatches sowie Codeüberwachung und -protokollierung. Sie müssen lediglich den Code angeben.

[AWS Step Functions](#)— AWS Step Functions macht es einfach, die Komponenten verteilter Anwendungen und Microservices mithilfe visueller Workflows zu koordinieren. Step Functions bietet eine grafische Konsole, mit der Sie die Komponenten Ihrer Anwendung in einer Reihe von Schritten anordnen und visualisieren können. Dies macht es einfach, mehrstufige Anwendungen zu erstellen und auszuführen. Step Functions startet und verfolgt jeden Schritt automatisch und versucht es erneut, wenn Fehler auftreten, sodass Ihre Anwendung ordnungsgemäß und wie erwartet ausgeführt wird.

Step Functions protokolliert den Status jedes Schritts, sodass Sie Probleme schnell diagnostizieren und debuggen können, wenn etwas schief geht. Sie können Schritte ändern und hinzufügen, ohne Code schreiben zu müssen, sodass Sie Ihre Anwendung weiterentwickeln und schneller innovieren können. AWS Step Functions ist Teil von AWS Serverless und macht es einfach, AWS Lambda Funktionen für serverlose Anwendungen zu orchestrieren. Sie können Step Functions auch für die Microservices-Orchestrierung mithilfe von Rechenressourcen wie Amazon EC2 und Amazon verwenden. ECS

[AWS Systems Manager](#) — AWS Systems Manager bietet Ihnen Transparenz und Kontrolle über Ihre Infrastruktur AWS. Systems Manager bietet eine einheitliche Benutzeroberfläche, über die Sie Betriebsdaten von mehreren AWS Diensten anzeigen können, und ermöglicht es Ihnen, betriebliche Aufgaben AWS ressourcenübergreifend zu automatisieren. Mit Systems Manager können Sie Ressourcen nach Anwendungen gruppieren, Betriebsdaten für die Überwachung und Fehlerbehebung anzeigen und auf Ihre Ressourcengruppen reagieren. Systems Manager kann Ihre Instanzen in ihrem definierten Zustand halten, bei Bedarf Änderungen vornehmen, z. B. Anwendungen aktualisieren oder Shell-Skripts ausführen, und andere Automatisierungs- und Patchaufgaben ausführen.

Sicherer Speicher

[Amazon Simple Storage Service](#) — Amazon S3 ist ein Objektspeicher, der darauf ausgelegt ist, beliebige Datenmengen von überall zu speichern und abzurufen. Er ist auf eine Beständigkeit von 99,999999999% ausgelegt und speichert Daten für Millionen von Anwendungen, die von Marktführern in allen Branchen verwendet werden. Amazon S3 bietet umfassende Sicherheit und wurde entwickelt, um Sie bei der Erfüllung Ihrer gesetzlichen Anforderungen zu unterstützen. Es bietet Kunden Flexibilität bei den Methoden, die sie zur Datenverwaltung zur Kostenoptimierung, Zugriffskontrolle und Einhaltung von Vorschriften verwenden. Amazon S3 bietet query-in-place Funktionen, mit denen Sie leistungsstarke Analysen direkt für Ihre in Amazon S3 gespeicherten Daten ausführen können. Amazon S3 ist ein stark unterstützter Cloud-Speicherservice, der von einer der größten Communitys von Drittanbieterlösungen, Systemintegrator-Partnern und anderen AWS Diensten integriert wird.

[Amazon S3 Glacier](#) — Amazon S3 Glacier ist ein sicherer, langlebiger und extrem kostengünstiger Cloud-Speicherservice für Datenarchivierung und Langzeitsicherung. Er ist auf eine Beständigkeit von 99,999999999% ausgelegt, bietet umfassende Sicherheit und wurde entwickelt, um Sie bei der Erfüllung Ihrer gesetzlichen Anforderungen zu unterstützen. S3 Glacier bietet query-in-place Funktionen, mit denen Sie leistungsstarke Analysen direkt für Ihre gespeicherten Archivdaten ausführen können. Um die Kosten niedrig zu halten und dennoch für unterschiedliche Abrufanforderungen geeignet zu sein, bietet S3 Glacier drei Optionen für den Zugriff auf Archive, von wenigen Minuten bis zu mehreren Stunden.

Künftige und maßgeschneiderte Sicherheitsfunktionen

Die oben genannten Dienste und Funktionen stellen keine vollständige Liste dar. AWS fügt ständig neue Funktionen hinzu. Weitere Informationen finden Sie auf den Seiten [Was ist neu bei AWS](#) und [AWS Cloud Security](#). Zusätzlich zu den Sicherheitsdiensten, die als native Cloud-Dienste AWS angeboten werden, könnten Sie daran interessiert sein, Ihre eigenen Funktionen zusätzlich zu den AWS Diensten aufzubauen.

Wir empfehlen zwar, einige grundlegende Sicherheitsdienste in Ihren Konten zu aktivieren, z. B. AWS CloudTrail Amazon und Amazon Macie GuardDuty, aber Sie möchten diese Funktionen möglicherweise erweitern, um zusätzlichen Nutzen aus Ihren Protokollbeständen zu ziehen. Es stehen eine Reihe von Partner-Tools zur Verfügung, wie sie beispielsweise in unserem Programm für APN Sicherheitskompetenz aufgeführt sind. Möglicherweise möchten Sie auch Ihre eigenen Abfragen schreiben, um Ihre Logs zu durchsuchen. Mit der großen Anzahl an verwalteten Diensten, die das AWS Unternehmen anbietet, war dies noch nie so einfach. Es gibt viele zusätzliche AWS

Dienste, die Sie bei Untersuchungen unterstützen können, die nicht in diesem paper werden, z. B. Amazon Athena, Amazon OpenSearch Service, Amazon QuickSight, Amazon Machine Learning und AmazonEMR.

Anhang B: Ressourcen zur Reaktion auf AWS Vorfälle

AWS veröffentlicht Ressourcen, um Kunden bei der Entwicklung von Funktionen zur Reaktion auf Vorfälle zu unterstützen. Die meisten Beispielcodes und Verfahren finden Sie im AWS externen GitHub öffentlichen Repository. Im Folgenden finden Sie einige Ressourcen mit Beispielen für die Reaktion auf Vorfälle.

Ressourcen aus dem Playbook

- [Framework for Incident Response Playbooks](#) — Ein Beispiel-Framework, mit dem Kunden Sicherheitsplaybooks erstellen, entwickeln und integrieren können, um sich auf mögliche Angriffsszenarien bei der Nutzung von Diensten vorzubereiten. AWS
- [Entwickeln Sie Ihre eigenen Incident-Response-Playbooks](#) — Dieser Workshop soll Ihnen helfen, sich mit der Entwicklung von Incident-Response-Playbooks für vertraut zu machen. AWS
- [Beispiele für Incident Response Playbooks](#) — Playbooks, die sich mit den häufigsten Szenarien befassen, mit denen Kunden konfrontiert sind. AWS
- [Erstellen eines AWS Incident-Response-Runbooks mithilfe von Jupyter-Playbooks und CloudTrail Lake](#) — Dieser Workshop führt Sie durch die Erstellung eines Incident-Response-Playbooks für Ihre Umgebung mithilfe von Jupyter-Notebooks und Lake. AWS CloudTrail

Forensische Ressourcen

- [Automatisiertes Framework zur Reaktion auf Vorfälle und Forensik](#) — Dieses Framework und die Lösung bieten einen standardmäßigen digitalen forensischen Prozess, der aus den folgenden Phasen besteht: Eindämmung, Erfassung, Untersuchung und Analyse. Es nutzt die Funktionen von AWS Lambda, um den Incident-Response-Prozess automatisiert und wiederholbar auszulösen. Es ermöglicht die Trennung von Konten, um die Automatisierungsschritte durchzuführen, Artefakte zu speichern und forensische Umgebungen zu erstellen.
- [Automated Forensics Orchestrator für Amazon EC2](#) — Dieser Implementierungsleitfaden bietet eine Self-Service-Lösung zur Erfassung und Untersuchung von Daten von EC2 Instances und angehängten Volumes für forensische Analysen, falls ein potenzielles Sicherheitsproblem entdeckt wird. Es gibt eine Vorlage für die Bereitstellung der Lösung AWS CloudFormation .

- [So automatisieren Sie die forensische Erfassung von Festplatten in AWS](#)— In diesem AWS Blog wird beschrieben, wie Sie einen Automatisierungsworkflow einrichten, um die Festplattennachweise für die Analyse zu erfassen und so den Umfang und die Auswirkungen potenzieller Sicherheitsvorfälle zu ermitteln. Es ist auch eine AWS CloudFormation Vorlage für die Bereitstellung der Lösung enthalten.

Hinweise

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

© 2024 Amazon Web Services, Inc. oder seine Tochtergesellschaften. Alle Rechte vorbehalten.

Dokumentverlauf

Änderung	Beschreibung	Datum
Aktualisiert: Aktualisierungen aufgrund von Kundenkommentaren zu Dokumenten.	<p>Aktualisiert https://docs.aws.amazon.com/security-ir/latest/userguide/setup — monitoring-and-investigation-workflows HTML zur Stackset-Vorlage.</p> <p>Die Einträge triage.security-ir.com bis triage.security-ir.amazonaws.com wurden korrigiert</p> <p>Hinweis zu verfolgten Verbindungen für -Contain auf .html hinzugefügt. AWSSupport EC2Reversible https://docs.aws.amazon.com/security-ir/latest/userguide/contain</p> <p>Fehlerhafter Link auf https://docs.aws.amazon.com/security-ir/latest/userguide/managing-associated-accounts.html behoben.</p> <p>Eine Definition für ein Mitgliedskonto wurde unter https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account.html hinzugefügt.</p> <p>Zu <a 750="" 918="" 934"="" 952="" data-label="Page-Footer" href="https://docs.aws.amazon.com/en_us/security-</p></td><td>20. Dezember 2024</td></tr></tbody></table></div><div data-bbox=">Version December 1, 2024 169</p>	

Änderung	Beschreibung	Datum
	ir/latest/userguide/using - service-linked-roles .html für AWS Organizations Verwaltungskonten wurde ein Hinweis zur Klarstellung hinzugefügt.	

Änderung	Beschreibung	Datum
<p>Aktualisiert: Aktualisierungen aufgrund von Kundenkommentaren zu Dokumenten.</p>	<p>Es wurden mehrere Duplikate AWS AWS im Text entfernt.</p> <p>Fehlerhafte Links auf https://docs.aws.amazon.com/security-ir/latest/userguide/sir_tagging.html and https://docs.aws.amazon.com/security-ir/latest/userguide/service-name-info-in-cloudtrail.html wurden behoben.</p> <p>Aktualisierungen für https://docs.aws.amazon.com/security-ir/latest/userguide/contain.html. Das > wurde aus dem ersten Absatz entfernt. AWSSupport-Contain wurde durch EC2Reversible-Contain AWSSupport ersetzt. EC2Instance-C durch AWSSupport-ContainIAMReversible ersetzt. AWSSupport containIAMPrincipal-Contains3Reversible wurde durch AWSSupport-contains3Resource ersetzt. AWSSupport</p> <p>Die Formatierung auf https://docs.aws.amazon.com/security-ir/latest/userguide/issues/en_us/ - .html wurde aktualisiert</p> <p>Wenn Kunden aufgefordert werden, CIRT über ein</p>	<p>10. Dezember 2024</p>

Änderung	Beschreibung	Datum
	<p>Support-Ticket Kontakt aufzunehmen, bietet https://docs.aws.amazon.com/security-ir/latest/userguide/understand-response-teams-and-support-.html nun Optionen zur Auswahl in den Support-Formularen.</p> <p>CloudWatch Ereignisse wurden entfernt und durch EventBridge on https://docs.aws.amazon.com/security-ir/latest/userguide/logging-and-events.html ersetzt.</p> <p>Grammatik-Updates auf https://docs.aws.amazon.com/security-ir/latest/userguide/technique-access-containment.html.</p> <p>Das Veröffentlichungsdatum wurde aus https://docs.aws.amazon.com/security-ir/latest/userguide/security-incident-response-guide-.html entfernt und durch Aktualisierungen in dieser Tabelle ersetzt.</p>	
Aktualisiert: AWS verwaltet Richtlinien und dienstbezogene Rollen.	Aktualisierungen der verwalteten Richtlinien und dienstbezogenen Rollen.	01. Dezember 2024

Änderung	Beschreibung	Datum
Servicestart	Erste Servicedokumente für die Einführung des Dienstes auf der re:Invent 2024	01. Dezember 2024

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.