



Benutzerhandbuch

Amazon Detective



Amazon Detective: Benutzerhandbuch

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

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen 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 Detective?	1
Funktionen von Amazon Detective	1
Zugreifen auf Amazon Detective	3
Preise für Amazon Detective	5
Wie funktioniert Detective?	5
Wer benutzt Detective?	6
Zugehörige Services	7
Erste Schritte	9
Bevor Sie beginnen	9
Melden Sie sich an für ein AWS-Konto	10
Erstellen Sie einen Benutzer mit Administratorzugriff	10
Voraussetzungen	11
Erteilung der erforderlichen Detective-Berechtigungen	12
Das Kontodatenvolumen muss innerhalb des Detective-Kontingents liegen	12
Unterstützte Version AWS Command Line Interface	12
Empfehlungen	12
Empfohlene Ausrichtung mit und GuardDuty AWS Security Hub	12
Es wird eine Aktualisierung der Benachrichtigungshäufigkeit empfohlen GuardDuty CloudWatch	13
Aktivieren von Detective	14
Detective aktivieren (Konsole)	14
Detective aktivieren (Detective API, AWS CLI)	15
Detective regionsübergreifend aktivieren (Python-Skript aktiviert GitHub)	15
Überprüfen, ob Daten extrahiert werden	16
Konzepte und Terminologie	17
Daten in einem Verhaltensdiagramm	22
Wie Amazon Detective Quelldaten verwendet, um ein Verhaltensdiagramm zu füllen	22
Wie Detective Quelldaten verarbeitet	23
Detective-Extraktion	23
Detective-Analysen	24
Trainingszeit für neue Verhaltensdiagramme	24
Überblick über die Datenstruktur des Verhaltensdiagramms	25
Arten von Elementen in der Datenstruktur des Verhaltensdiagramms	25
Arten von Entitäten in der Datenstruktur des Verhaltensdiagramms	26

In einem Verhaltensdiagramm verwendete Quelldaten	31
Arten von Kerndatenquellen in Detective	32
Arten optionaler Datenquellen in Detective	33
Amazon EKS-Auditprotokolle für Detective	34
AWS Ergebnisse zur Sicherheit	35
Wie Detective Quelldaten aufnimmt und speichert	36
Wie Detective das Datenvolumenkontingent für Verhaltensdiagramme durchsetzt	37
Wie Detective für Ermittlungen eingesetzt wird	38
Detective Untersuchung	38
Durchführung einer Detective Untersuchung	39
Überprüfen von Untersuchungsberichten	42
Einen Detective Investigations-Bericht verstehen	43
Übersicht des Untersuchungsberichts	44
Untersuchungsbericht herunterladen	45
Archivieren eines Untersuchungsberichts	46
Ermittlungsphasen und Ausgangspunkte	46
Phasen der Untersuchung	46
Ausgangspunkte für eine Detective Untersuchung	47
Ablauf der detektivischen Ermittlungen	49
Analyse der Ergebnisse	51
Überblick über Erkenntnisse	51
Zeitbereich, der für die Erkenntnisübersicht verwendet wurden	51
Erkenntnisdetails	52
Verbundene Entitäten	52
Problembehandlung bei „Seite nicht gefunden“	52
Gruppen finden	53
Grundlegendes zur Seite „Erkenntnisgruppen“	54
Informative Erkenntnisse in Erkenntnisgruppen	56
Gruppenprofile finden	57
Visualisierung von Erkenntnisgruppen	59
Erkenntnisgruppenübersicht	61
Erkenntnisgruppenübersichten überprüfen	62
Die Übersicht der Erkenntnisgruppe wird deaktiviert	63
Die Erkenntnisgruppenübersicht wird aktiviert	64
Unterstützte Regionen	64
Entitäten analysieren	65

Verwenden der Seite „Übersicht“	65
Untersuchungen	66
Neu beobachtete Geolocations	67
Aktive Erkenntnisgruppen in den letzten 7 Tagen	67
Rollen und Benutzer mit dem höchsten API-Aufrufvolumen	68
EC2-Instances mit dem höchsten Verkehrsvolumen	68
Container-Cluster mit den meisten Kubernetes-Pods	69
Benachrichtigung über den ungefähren Wert	69
Verwenden von Entitätsprofilen	70
Geltungsbereich eines Entitätsprofils	70
Kennung und Typ der Entität	71
Involvierte Erkenntnisse	71
Erkenntnisgruppen, an denen diese Entität beteiligt ist	71
Profilbereich mit Entitätsdetails und Analyseergebnissen	71
In einem Entitätsprofil navigieren	72
Profilbereich anzeigen und mit ihnen interagieren	72
Inhalt des Profilbereichs	73
Einstellungen für Profilbereiche	82
Zu einer anderen Konsole wechseln	83
Zu einem anderen Entitätsprofil wechseln	84
Erkunden von Aktivitätsdetails	84
Direkt zu einem Entitätsprofil navigieren oder eine Übersicht finden	106
Von einer anderen Konsole aus wechseln	106
Navigation mithilfe einer URL	108
Hinzufügen von Detective-URLs für Erkenntnisse zu Splunk	112
Verwaltung des Zeitbereichs	112
Festlegen des spezifischen Start- und Enddatums und der Uhrzeiten	113
Bearbeiten der Zeitdauer für den Zeitbereich	114
Stellen Sie den Zeitbereich auf ein Zeitfenster für die Suche ein	114
Festlegen des Zeitbereichs auf der Übersichtsseite	115
Erkenntnisse für eine Entität anzeigen	115
Entitäten mit hohem Volumen	116
Was ist eine Entität mit hohem Volumen?	116
Anzeige der Benachrichtigung über Entitäten mit hohem Volumen in einem Profil	117
Die Liste der Entitäten mit hohem Volumen für den aktuellen Gültigkeitszeitraum anzeigen .	118
Verwaltung von Ergebnissen und Entitäten	119

Suche nach einer Erkenntnis oder Entität	119
Abschließen der Suche	119
Verwenden der Suchergebnisse	121
Fehlerbehebung bei der Suche	122
Exportieren von Daten aus Detective	122
Archivierung eines GuardDuty Befundes	123
Verwalten von Konten	124
Beschränkungen und Empfehlungen	125
Maximale Anzahl von Mitgliedern pro Konto	125
Konten und Regionen	125
Abstimmung der Administratorkonten mit Security Hub und GuardDuty	125
Gewährung der erforderlichen Berechtigungen für Administratorkonten	126
Reflektieren von Organisationsaktualisierungen in Detective	126
Der Übergang zu Organizations	126
Festlegen eines Detective-Administratorkontos für Ihre Organisation	127
Organisationskonten als Mitgliedskonten aktivieren	127
Festlegen des Detective-Administratorkontos	128
So wird das Detective-Administratorkonto verwaltet	128
Erforderliche Berechtigungen zur Konfiguration des Detective-Administratorkontos	130
Festlegen eines Detective-Administratorkontos (Konsole)	130
Benennen eines Detective-Administratorkontos (Detective API, AWS CLI)	133
Entfernen eines Detective-Administratorkontos (Konsole)	133
Das Detective-Administratorkonto entfernen (Detective API, AWS CLI)	134
Das delegierte Administratorkonto entfernen (Organizations API, AWS CLI)	135
Verfügbare Aktionen für Konten	136
Anzeige der Kontenliste	137
Auflisten von Konten (Konsole)	139
Deine Mitgliedskonten auflisten (Detective API, AWS CLI)	140
Mitgliedskonten von Organisationen verwalten	141
Neue Organisationskonten automatisch aktivieren	142
Organisationskonten als Mitgliedskonten aktivieren	144
Aufheben der Zuordnung von Organisationskonten	146
Verwaltung eingeladener Konten	147
Mitgliedskonten zu einem Verhaltensdiagramm einladen	147
Aktivierung eines Mitgliedskontos, das nicht aktiviert ist	153
Mitgliedskonten aus einem Verhaltensdiagramm entfernen	154

Für Mitgliedskonten: Einladungen und Mitgliedschaften verwalten	156
IAM-Richtlinie für ein Mitgliedskonto	157
Einladungen in Verhaltensdiagrammen anzeigen	158
Auf eine Einladung zu einem Verhaltensdiagramm antworten	159
Ihr Konto aus einem Verhaltensdiagramm entfernen	161
Auswirkung von Kontoaktionen	162
Detective deaktiviert	162
Das Mitgliedskonto wird aus dem Verhaltensdiagramm entfernt.	163
Das Mitgliedskonto verlässt die Organisation	163
AWS Konto gesperrt	163
AWS Konto geschlossen	163
Amazon Detective Python-Skripte	164
Überblick über das Skript <code>enableDetective.py</code>	165
Überblick über das Skript <code>disableDetective.py</code>	165
Erforderliche Berechtigungen für die Skripts	166
Einrichtung der Ausführungsumgebung für die Python-Skripte	167
Erstellen einer <code>.csv</code> -Liste von Mitgliedskonten, die hinzugefügt oder entfernt werden sollen	169
Ausführen von <code>enableDetective.py</code>	170
Ausführen von <code>disableDetective.py</code>	171
Integration mit Amazon Security Lake	173
Bevor Sie beginnen	175
Schritt 1: Erstellen eines Security Lake-Abonnenten	175
Schritt 2: Fügen Sie die erforderlichen IAM-Berechtigungen zu Ihrem Konto hinzu	176
Schritt 3: Annahme der Resource Share ARN-Einladung und Aktivieren der Integration	179
Erstellen eines Stacks mithilfe der AWS CloudFormation -Vorlage	179
Einen CloudFormation Stack löschen	186
Ändern der Integrationskonfiguration	187
Deaktivierung der Integration	188
Unterstützte AWS Regionen	188
Abfragen von Rohprotokollen in Detective	190
Fragen Sie Rohprotokolle für eine AWS Rolle ab	193
Rohprotokolle für einen Amazon EKS-Cluster abfragen	194
Abfragen von Rohprotokollen für eine Amazon-EC2-Instance	194
Sicherheit	196
Datenschutz	197

Schlüsselverwaltung	198
Identity and Access Management	198
Zielgruppe	199
Authentifizierung mit Identitäten	199
Verwalten des Zugriffs mit Richtlinien	203
So funktioniert Amazon Detective mit IAM	206
Beispiele für identitätsbasierte Richtlinien	213
AWS verwaltete Richtlinien	219
Verwenden von serviceverknüpften Rollen	230
Fehlerbehebung für -Identität und -Zugriff	233
Protokollierung und Überwachung	235
Compliance-Validierung	235
Ausfallsicherheit	236
Sicherheit der Infrastruktur	236
Bewährte Methoden für die Gewährleistung der Sicherheit	237
Best Practices für Administratorkonten	237
Bewährte Methoden für Mitgliedskonten	237
Prognose und Überwachung der Kosten	238
Über die kostenlose Testversion für Verhaltensdiagramme	238
Kostenlose Testversion für optionale Datenquellen	239
Nutzung und Kosten des Administratorkontos	240
Volumen der für jedes Konto aufgenommenen Daten	240
Voraussichtliche Kosten für das Verhaltensdiagramm	241
Voraussichtliche Kosten für das Verhaltensdiagramm	241
Menge der von Quellpaketen aufgenommenen Daten	242
Nachverfolgung der Nutzung von Mitgliedskonten	242
Aufgenommenes Volumen für jedes Verhaltensdiagramm	243
Prognostizierte Kosten für alle Verhaltensdiagramme	243
Wie Detective die voraussichtlichen Kosten berechnet	243
Detective API-Aufrufe protokollieren mit CloudTrail	245
Detektivinformationen in CloudTrail	245
Grundlagen zu Protokolldateieinträgen in Detective	246
Regionen und Kontingente	248
Detective-Regionen und -Endpunkte	248
Kontingente von Detective	248
Internet Explorer 11 wird nicht unterstützt	249

Verwalten von Tags	250
Die Tags für ein Verhaltensdiagramm anzeigen (Konsole)	250
Auflisten der Tags für ein Verhaltensdiagramm (Detective API, AWS CLI)	250
Hinzufügen von Tags zu einem Verhaltensdiagramm (Konsole)	251
Hinzufügen von Tags zu einem Verhaltensdiagramm (Detective API, AWS CLI)	251
Tags aus einem Verhaltensdiagramm entfernen (Konsole)	252
Tags aus einem Verhaltensdiagramm entfernen (Detective API, AWS CLI)	252
Deaktivieren von Amazon Detective	253
Detective deaktivieren (Konsole)	253
Detective deaktivieren (Detective API, AWS CLI)	253
Detective regionsübergreifend deaktivieren (Python-Skript aktiviert GitHub)	254
Dokumentverlauf	255
.....	cclxxxiii

Was ist Amazon Detective?

Amazon Detective hilft Ihnen, die Ursache von Sicherheitserkenntnissen oder verdächtigen Aktivitäten zu analysieren, zu untersuchen und schnell zu identifizieren. Detective sammelt automatisch Protokolldaten aus Ihren AWS -Ressourcen. Es verwendet dann Machine Learning, statistische Analysen und die Diagrammtheorie, um Visualisierungen zu erstellen, mit denen Sie effektive Sicherheitsuntersuchungen schneller und effizienter durchführen können. Detective bietet vordefinierte Datenaggregationen, Übersichten und Kontexte, mit denen Sie Art und Ausmaß möglicher Sicherheitsprobleme schnell analysieren und feststellen können.

Mit Detective können Sie auf historische Ereignisdaten von bis zu einem Jahr zugreifen. Diese Daten sind über eine Reihe von Visualisierungen verfügbar, die Veränderungen in Art und Umfang der Aktivitäten in einem ausgewählten Zeitfenster zeigen. Detective verknüpft diese Änderungen mit GuardDuty Ergebnissen. Weitere Informationen zu Quelldaten in Detective finden Sie unter [the section called “In einem Verhaltensdiagramm verwendete Quelldaten”](#).

Durch die automatische Aggregation von Daten und die Bereitstellung visueller Tools können Sie mit Amazon Detective schnellere und effizientere Sicherheitsuntersuchungen durchführen. Sie können potenzielle Probleme schnell analysieren und den Umfang der Sicherheitsbedrohungen ermitteln.

Themen

- [Funktionen von Amazon Detective](#)
- [Zugreifen auf Amazon Detective](#)
- [Preise für Amazon Detective](#)
- [Wie funktioniert Detective?](#)
- [Wer benutzt Detective?](#)
- [Zugehörige Services](#)

Funktionen von Amazon Detective

Im Folgenden finden Sie einige der wichtigsten Möglichkeiten, wie Amazon Detective bei der Untersuchung verdächtiger Aktivitäten in Ihrer AWS Umgebung und bei der Analyse von Ressourcen hilfreich ist, um die Hauptursache von Sicherheitsproblemen zu ermitteln.

Detective finden Gruppen

Mithilfe von [Detective Finding Groups](#) können Sie mehrere Aktivitäten untersuchen, die sich auf ein potenzielles Sicherheitsereignis beziehen. Mithilfe von Suchgruppen können Sie die Grundursache für GuardDuty Ergebnisse mit hohem Schweregrad analysieren. Wenn ein Bedrohungsakteur versucht, Ihre AWS Umgebung zu kompromittieren, führt er in der Regel eine Abfolge von Aktionen durch, die zu mehreren Sicherheitsergebnissen und ungewöhnlichem Verhalten führen.

Auf der Seite „Suchgruppen“ in Detective werden alle zugehörigen Findungsgruppen angezeigt, die aus Ihrem Verhaltensdiagramm auf der Seite „Suchgruppen“ extrahiert wurden. Sie können [Beweise](#) für verschiedene Prinzipaltypen (wie IAM-Benutzer oder IAM-Rolle) beobachten. Bei einigen Arten von Nachweisen können Sie Beweise für alle Konten beobachten.

Detective bietet eine interaktive Visualisierung jeder Findungsgruppe, damit Sie Sicherheitsprobleme schneller und gründlicher untersuchen können. Die Visualisierung ist so konzipiert, dass Entitäten und Ergebnisse angezeigt werden, die an einem Sicherheitsvorfall beteiligt waren, sodass Zusammenhänge und Ursachen leichter zu verstehen sind. Sie können Probleme schneller und gründlicher mit weniger Aufwand untersuchen. Im Bereich [Visualisierung von Erkenntnisgruppen](#) werden die Erkenntnisse und Entitäten angezeigt, die an einer Erkenntnisgruppe beteiligt sind.

Detective Investigation zur Triage der Ergebnisse

Mit [Detective Investigation](#) können Sie IAM-Benutzer und IAM-Rollen anhand von Bedrohungsindikatoren untersuchen, anhand derer Sie feststellen können, ob eine Ressource an einem Sicherheitsvorfall beteiligt ist. 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. Mit Detective Investigations können Sie die Effizienz maximieren, sich auf Sicherheitsbedrohungen konzentrieren und die Reaktionsfähigkeit auf Vorfälle verbessern.

Detective Investigation verwendet Modelle für maschinelles Lernen und Bedrohungsinformationen, um nur die kritischsten, verdächtigsten Probleme aufzudecken, sodass Sie sich auf hochrangige Untersuchungen konzentrieren können. Es analysiert automatisch die Ressourcen in Ihrer AWS Umgebung, um potenzielle Anzeichen für kompromittierte oder verdächtige Aktivitäten zu identifizieren. Auf diese Weise können Sie Muster erkennen und nachvollziehen, welche Ressourcen von Sicherheitsereignissen betroffen sind, was einen proaktiven Ansatz zur Identifizierung und Abwehr von Bedrohungen bietet.

Sie können „Detective Investigation“ von der Detective-Konsole aus starten verwenden, indem Sie [„Detective Investigation“ ausführen](#). Verwenden Sie den [StartInvestigation](#) Betrieb der Detective-API, um eine Untersuchung programmgesteuert durchzuführen. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [start-investigation](#) aus.

Detective-Integration mit Amazon Security Lake

[Detective ist in Amazon Security Lake integriert](#), was bedeutet, dass Sie die von Security Lake gespeicherten Rohprotokolldaten abfragen und abrufen können. Mit dieser Integration können Sie Protokolle und Ereignisse aus den folgenden Quellen sammeln, die Security Lake nativ unterstützt.

- AWS CloudTrail Verwaltungsereignisse
- Amazon Virtual Private Cloud (Amazon VPC)-Datendurchflussprotokolle

Nachdem Sie Detective in Security Lake integriert haben, beginnt Detective mit dem Abrufen von Rohprotokollen aus Security Lake, die sich auf AWS CloudTrail Verwaltungsereignisse und Amazon VPC Flow Logs beziehen. Sie können [Rohprotokolle abfragen](#), um die Protokolle und Ereignisse in Detective anzuzeigen.

Untersuchen Sie das VPC-Durchflussvolumen

Mit Detective können Sie interaktiv die [Aktivitätsdetails der Virtual Private Cloud \(VPC\) - Netzwerkflüsse](#) Ihrer Amazon Elastic Compute Cloud (Amazon EC2) -Instances und Kubernetes-Pods untersuchen. Detective sammelt automatisch VPC-Flow-Logs von Ihren überwachten Konten, aggregiert sie nach EC2-Instances und präsentiert visuelle Zusammenfassungen und Analysen zu diesen Netzwerkflüssen.

Für eine EC2-Instance zeigen die Aktivitätsdetails für das Gesamte VPC-Datendurchflussvolumen die Interaktionen zwischen der EC2-Instance und IP-Adressen während eines ausgewählten Zeitraums.

Für einen Kubernetes-Pod zeigt Gesamtes VPC-Datendurchflussvolumen das Gesamtvolumen der Bytes an, die in die zugewiesene IP-Adresse des Kubernetes-Pods für alle Ziel-IP-Adressen ein- und ausgehen.

Zugreifen auf Amazon Detective

Amazon Detective ist in den meisten Fällen verfügbar AWS-Regionen. Eine Liste der Regionen, in denen Detective derzeit verfügbar ist, finden Sie unter [Amazon Detective Endpoints and Quotas](#) in

der Allgemeine AWS-Referenz. Informationen zur Verwaltung AWS-Regionen für Sie finden Sie im AWS Account Management Referenzhandbuch unter [Spezifizieren AWS-Konto, welche Konten für AWS-Regionen Ihr Konto verwendet werden können](#).

In jeder Region können Sie auf eine der folgenden Arten mit Detective zusammenarbeiten.

AWS Management Console

Das AWS Management Console ist eine browserbasierte Oberfläche, mit der Sie AWS Ressourcen erstellen und verwalten können. Als Teil dieser Konsole bietet die Amazon Detective-Konsole Zugriff auf Ihr Detective-Konto, Ihre Daten und Ressourcen. Mit der Detective Console können Sie jede Detective-Aufgabe ausführen: Überprüfen Sie potenzielle Sicherheitsbedrohungen und analysieren, untersuchen und identifizieren Sie die Hauptursache von Sicherheitslücken.

AWS Befehlszeilentools

Mit AWS Befehlszeilentools können Sie Befehle an der Befehlszeile Ihres Systems ausgeben, um Detective-Aufgaben und AWS -Aufgaben auszuführen. Die Verwendung der Befehlszeile kann schneller und bequemer sein als die Verwendung der Konsole. Die Befehlszeilen-Tools können auch beim Erstellen von Skripts für -Aufgaben hilfreich sein.

AWS stellt zwei Gruppen von Befehlszeilentools bereit: das AWS Command Line Interface (AWS CLI) und das AWS Tools for PowerShell. Informationen zur Installation und Verwendung von finden Sie im [AWS Command Line Interface Benutzerhandbuch](#). AWS CLI Informationen zur Installation und Verwendung der Tools für PowerShell finden Sie im [AWS Tools for PowerShell Benutzerhandbuch](#).

AWS SDKs

AWS stellt SDKs bereit, die aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen bestehen, z. B. Java, Go, Python, C++ und .NET. Die SDKs bieten bequemen, programmatischen Zugriff auf Detective und andere AWS-Services Sie übernehmen auch Aufgaben wie das kryptografische Signieren von Anfragen, das Verwalten von Fehlern und das automatische Wiederholen von Anfragen. Informationen zur Installation und Verwendung der AWS SDKs finden Sie unter [Tools](#) to Build On. AWS

Amazon Detective REST-API

Die Amazon Detective REST-API bietet Ihnen umfassenden, programmatischen Zugriff auf Ihr Detective-Konto, Ihre Daten und Ressourcen. Mit dieser API können Sie HTTPS-Anfragen direkt

an Detective senden. Im Gegensatz zu den AWS Befehlszeilentools und SDKs erfordert die Verwendung dieser API jedoch, dass Ihre Anwendung Details auf niedriger Ebene verarbeitet, z. B. die Generierung eines Hashs zum Signieren einer Anfrage. Informationen zu dieser API finden Sie in der [Detective API-Referenz](#).

Preise für Amazon Detective

Wie bei anderen AWS Produkten gibt es keine Verträge oder Mindestverpflichtungen für die Nutzung von Amazon Detective.

Die Preisgestaltung von Detective basiert auf mehreren Dimensionen — und berechnet eine gestaffelte Flatrate pro GB für alle Daten, unabhängig von der Quelle. Weitere Informationen finden Sie unter [Amazon Detective — Preise](#).

Damit Sie die Kosten für die Nutzung von Detective besser verstehen und prognostizieren können, gibt Detective die geschätzten Nutzungskosten für Ihr Konto an. Sie können [diese Schätzungen in der Amazon Detective-Konsole überprüfen](#) und mit der Amazon Detective API darauf zugreifen. Je nachdem, wie Sie den Dienst nutzen, können zusätzliche Kosten für die Nutzung anderer Dienste AWS-Services in Kombination mit bestimmten Detective-Funktionen wie der Security Lake-Integration und Detective Investigations anfallen.

Wenn Sie Detective zum ersten Mal aktivieren, nehmen Sie AWS-Konto automatisch an der kostenlosen 30-Tage-Testversion von Detective teil. Dies schließt einzelne Konten ein, die als Teil einer Organisation in aktiviert wurden. AWS Organizations Während der kostenlosen Testversion fallen für die Nutzung von Detective in den jeweiligen Fällen keine Gebühren an AWS-Region.

Um Ihnen zu helfen, die Kosten für die Nutzung von Detective nach Ablauf der kostenlosen Testversion zu verstehen und zu prognostizieren, gibt Ihnen Detective die geschätzten Nutzungskosten, die auf Ihrer Nutzung von Detective während der Testphase basieren. Ihre Nutzungsdaten geben auch an, wie viel Zeit bis zum Ende Ihrer kostenlosen Testversion noch verbleibt. Sie können [diese Daten in der Amazon Detective-Konsole überprüfen](#) und mit der Amazon Detective API darauf zugreifen.

Wie funktioniert Detective?

Detective extrahiert automatisch zeitbasierte Ereignisse wie Anmeldeversuche, API-Aufrufe und Netzwerkverkehr aus AWS CloudTrail den Amazon VPC-Flussprotokollen. Es nimmt auch Ergebnisse auf, die von erkannt wurden. GuardDuty

Detective nutzt Machine Learning und Visualisierung auf Grundlage dieser Ereignisse, um eine einheitliche, interaktive Ansicht des Ressourcenverhaltens und der Interaktionen zwischen ihnen im Zeitverlauf zu erstellen. Sie können dieses Verhaltensdiagramm untersuchen, um verschiedene Aktionen wie fehlgeschlagene Anmeldeversuche oder verdächtige API-Aufrufe zu untersuchen. Sie können auch sehen, wie sich diese Aktionen auf Ressourcen wie AWS Konten und Amazon EC2 EC2-Instances auswirken. Sie können den Umfang und den Zeitplan des Verhaltensdiagramms für eine Vielzahl von Aufgaben anpassen:

- Untersuchen Sie schnell alle Aktivitäten, die nicht der Norm entsprechen.
- Identifizieren Sie Muster, die auf ein Sicherheitsproblem hinweisen könnten.
- Machen Sie sich mit allen Ressourcen vertraut, die von einer Erkenntnis betroffen sind.

Maßgeschneiderte Visualisierungen von Detective bieten eine Grundlage für die Kontoinformationen und fassen sie zusammen. Diese Erkenntnisse können helfen, Fragen wie „Ist das ein ungewöhnlicher API-Aufruf für diese Rolle?“ zu beantworten. Oder „Wird dieser Anstieg des Datenverkehrs von dieser Instance erwartet?“

Mit Detective müssen Sie keine Daten organisieren oder Ihre eigenen Abfragen und Algorithmen entwickeln, konfigurieren oder optimieren. Es fallen keine Vorabkosten an und Sie zahlen nur für die analysierten Ereignisse. Sie müssen keine zusätzliche Software bereitstellen oder andere Feeds abonnieren.

Wer benutzt Detective?

Wenn Detective für ein Konto aktiviert wird, wird es zum Administratorkonto für ein Verhaltensdiagramm. Ein Verhaltensdiagramm ist ein verknüpfter Satz extrahierter und analysierter Daten aus einem oder mehreren AWS Konten. Administratorkonten laden Mitgliedskonten ein, ihre Daten zum Verhaltensdiagramm des Administratorkontos beizutragen.

Detective ist auch in integriert AWS Organizations. Das Verwaltungskonto Ihrer Organisation wird als Detective-Administratorkonto für die Organisation festgelegt. Das Detective-Administratorkonto aktiviert Organisationskonten als Mitgliedskonten im Diagramm zum Organisationsverhalten.

Informationen darüber, wie Detective Quelldaten von Verhaltensdiagrammkonten verwendet, finden Sie unter [the section called “In einem Verhaltensdiagramm verwendete Quelldaten”](#).

Informationen darüber, wie Administratorkonten Verhaltensdiagramme verwalten, finden Sie unter [Verwalten von Konten](#). Informationen darüber, wie Mitgliedskonten Einladungen und Mitgliedschaften

in Verhaltensdiagrammen verwalten, finden Sie unter [the section called “Für Mitgliedskonten: Einladungen und Mitgliedschaften verwalten”](#).

Das Administratorkonto verwendet die aus dem Verhaltensdiagramm generierten Analysen und Visualisierungen, um AWS Ressourcen und GuardDuty Ergebnisse zu untersuchen. Mithilfe der Detective-Integrationen mit GuardDuty und AWS Security Hub können Sie von einem GuardDuty Ergebnis in diesen Diensten direkt zur Detective-Konsole wechseln.

Eine Untersuchung in Detective konzentriert sich auf die Aktivität, die mit den beteiligten AWS - Ressourcen verbunden ist. Einen Überblick über den Ermittlungsprozess in Detective finden Sie im Detective-Benutzerhandbuch unter [Wie Amazon Detective für Ermittlungen verwendet wird](#).

Zugehörige Services

Um Ihre Daten, Workloads und Anwendungen weiter zu schützen, sollten Sie erwägen AWS, Folgendes AWS-Services in Kombination mit Amazon Detective zu verwenden.

AWS Security Hub

AWS Security Hub bietet Ihnen einen umfassenden Überblick über den Sicherheitsstatus Ihrer AWS Ressourcen und hilft Ihnen dabei, Ihre AWS Umgebung anhand von Industriestandards und Best Practices zu überprüfen. Dies geschieht unter anderem dadurch, dass Ihre Sicherheitsergebnisse aus mehreren AWS-Services (einschließlich Detective) und unterstützten AWS Partner Network (APN) -Produkten (einschließlich Detective) verarbeitet, aggregiert, organisiert und priorisiert werden. Security Hub hilft Ihnen dabei, Ihre Sicherheitstrends zu analysieren und die Sicherheitsprobleme mit der höchsten Priorität in Ihrer AWS Umgebung zu identifizieren.

Weitere Informationen zu Security Hub finden Sie im [AWS Security Hub Benutzerhandbuch](#).

Amazon GuardDuty

Amazon GuardDuty ist ein Sicherheitsüberwachungsdienst, der bestimmte Arten von AWS Protokollen analysiert und verarbeitet, z. B. AWS CloudTrail Datenereignisprotokolle für Amazon S3 und CloudTrail Verwaltungsereignisprotokolle. Er verwendet Feeds mit Bedrohungsinformationen wie Listen bössartiger IP-Adressen und Domänen sowie maschinelles Lernen, um unerwartete und potenziell unautorisierte und bössartige Aktivitäten in Ihrer AWS Umgebung zu identifizieren.

Weitere Informationen GuardDuty finden Sie im [GuardDuty Amazon-Benutzerhandbuch](#).

Amazon Security Lake

Amazon Security Lake ist ein vollständig verwalteter Sicherheits-Data-Lake-Dienst. Sie können Security Lake verwenden, um Sicherheitsdaten aus AWS Umgebungen, SaaS-Anbietern, lokalen Quellen, Cloud-Quellen und Quellen von Drittanbietern automatisch in einem speziell entwickelten Data Lake zu zentralisieren, der in Ihrem Konto gespeichert wird. AWS Security Lake hilft Ihnen bei der Analyse von Sicherheitsdaten, sodass Sie sich ein umfassenderes Bild von der Sicherheitslage in Ihrem gesamten Unternehmen machen können. Mit Security Lake können Sie auch den Schutz Ihrer Workloads, Anwendungen und Daten verbessern.

Weitere Informationen zu Security Lake finden Sie im [Amazon Security Lake-Benutzerhandbuch](#). Weitere Informationen zur gemeinsamen Verwendung von Detective und Security Lake finden Sie unter [Integration mit Amazon Security Lake](#).

Weitere Informationen zu zusätzlichen AWS Sicherheitsservices finden Sie unter [Sicherheit, Identität und Compliance auf AWS](#).

Erste Schritte mit Amazon Detective

Dieses Tutorial bietet eine Einführung in Amazon Detective. Sie erfahren, wie Sie Detective für Ihr AWS Konto aktivieren. Sie erfahren auch, wie Sie überprüfen können, ob Detective damit begonnen hat, Daten aus Ihrem AWS Konto aufzunehmen und in Ihr Verhaltensdiagramm zu extrahieren.

Wenn Sie Amazon Detective aktivieren, erstellt Detective ein regionspezifisches Verhaltensdiagramm, das Ihr Konto als Administratorkonto verwendet. Dies ist zunächst das einzige Konto im Verhaltensdiagramm. Das Administratorkonto kann dann andere AWS Konten einladen, ihre Daten zum Verhaltensdiagramm beizutragen. Siehe [Verwalten von Konten](#).

Wenn Sie Detective in einer Region zum ersten Mal aktivieren, beginnt auch eine kostenlose 30-Tage-Testversion für das Verhaltensdiagramm. Wenn das Konto Detective deaktiviert und dann wieder aktiviert, ist keine kostenlose Testversion verfügbar. Siehe [the section called “Über die kostenlose Testversion für Verhaltensdiagramme”](#).

Nach der kostenlosen Testversion werden jedem Konto im Verhaltensdiagramm die Daten in Rechnung gestellt, die es dazu beiträgt. Das Administratorkonto kann die Nutzung verfolgen und die voraussichtlichen Gesamtkosten für einen typischen Zeitraum von 30 Tagen für das gesamte Verhaltensdiagramm einsehen. Weitere Informationen finden Sie unter [the section called “Nutzung und Kosten des Administratorkontos”](#). Mitgliedskonten können die Nutzung und die voraussichtlichen Kosten der Verhaltensdiagramme, zu denen sie gehören, verfolgen. Weitere Informationen finden Sie unter [the section called “Nachverfolgung der Nutzung von Mitgliedskonten”](#).

Themen

- [Bevor Sie beginnen](#)
- [Voraussetzungen](#)
- [Empfehlungen](#)
- [Aktivieren von Amazon Detective](#)
- [Überprüfen, ob Daten extrahiert werden](#)

Bevor Sie beginnen

Bevor Sie Amazon Detective aktivieren können, müssen Sie über eine AWS-Konto verfügen.

Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie <https://portal.aws.amazon.com/billing/signup>.
2. Folgen Sie den Online-Anweisungen.

Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontos wird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um [Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich](#) ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu <https://aws.amazon.com/> auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich [AWS Management Console](#) als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter [Anmelden als Root-Benutzer](#) im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

Anweisungen finden Sie unter [Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer \(Konsole\)](#) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

Anweisungen finden Sie unter [Aktivieren AWS IAM Identity Center](#) im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden [Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis](#) im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie [im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal](#).

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

Anweisungen finden Sie im Benutzerhandbuch unter [Einen Berechtigungssatz erstellen](#).AWS IAM Identity Center

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

Anweisungen finden [Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen](#).

Voraussetzungen

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind.

Erteilung der erforderlichen Detective-Berechtigungen

Bevor Sie Detective aktivieren können, müssen Sie sicherstellen, dass Ihr IAM-Prinzipal über die erforderlichen Detective-Berechtigungen verfügt. Der Prinzipal kann ein vorhandener Benutzer oder eine bestehende Rolle sein, die Sie bereits verwenden, oder Sie können einen neuen Benutzer oder eine neue Rolle für Detective erstellen.

Bei der Registrierung für Amazon Web Services (AWS) wird Ihr Konto automatisch für alle AWS-Services registriert, einschließlich Amazon Detective. Um Detective zu aktivieren und zu verwenden, müssen Sie jedoch zunächst Berechtigungen einrichten, die Ihnen den Zugriff auf die Amazon-Detective-Konsole und API-Vorgänge ermöglichen. Sie oder Ihr Administrator können dies tun, indem Sie AWS Identity and Access Management (IAM) verwenden, um die [AmazonDetectiveFullAccessverwaltete Richtlinie](#) an Ihren IAM-Prinzipal anzuhängen, der Zugriff auf alle Detective-Aktionen gewährt.

Das Kontodatenvolumen muss innerhalb des Detective-Kontingents liegen

Das Datenvolumen, das in ein Verhaltensdiagramm fließt, muss unter dem zulässigen Höchstwert von Detective liegen.

Wenn Sie versuchen, Detective zu aktivieren und das Datenvolumen für Ihr Konto zu groß ist, können Sie Detective nicht aktivieren. In der Detective-Konsole wird eine Benachrichtigung angezeigt, die darauf hinweist, dass das Datenvolumen zu groß ist.

Unterstützte Version AWS Command Line Interface

Um die AWS CLI zur Ausführung von Detective-Aufgaben verwenden zu können, ist mindestens Version 1.16.303 erforderlich.

Empfehlungen

Empfohlene Ausrichtung mit und GuardDuty AWS Security Hub

Wenn Sie bei GuardDuty und registriert sind AWS Security Hub, empfehlen wir, dass Ihr Konto ein Administratorkonto für diese Dienste ist. Wenn die Administratorkonten für alle drei Dienste identisch sind, funktionieren die folgenden Integrationspunkte problemlos.

- In GuardDuty unserem Security Hub können Sie beim Anzeigen von Details zu einem GuardDuty Befund von den Befunddetails zum Detective-Findungsprofil wechseln.

- In Detective können Sie bei der Untersuchung eines GuardDuty Befundes die Option wählen, dieses Ergebnis zu archivieren.

Wenn Sie unterschiedliche Administratorkonten für GuardDuty und Security Hub haben, empfehlen wir Ihnen, die Administratorkonten auf den Dienst abzustimmen, den Sie häufiger verwenden.

- Wenn Sie GuardDuty häufiger verwenden, aktivieren Sie Detective über das GuardDuty Administratorkonto.

Wenn Sie Konten verwalten AWS Organizations , legen Sie das GuardDuty Administratorkonto als Detective-Administratorkonto für die Organisation fest.

- Wenn Sie Security Hub häufiger verwenden, aktivieren Sie Detective über das Security Hub-Administratorkonto.

Wenn Sie Organizations zur Verwaltung von Konten verwenden, legen Sie das Security Hub-Administratorkonto als Detective-Administratorkonto für die Organisation fest.

Wenn Sie nicht dieselben Administratorkonten für alle Dienste verwenden können, können Sie nach der Aktivierung von Detective optional eine kontoübergreifende Rolle erstellen. Diese Rolle gewährt einem Administratorkonto Zugriff auf andere Konten.

Informationen dazu, wie IAM diese Art von Rolle unterstützt, finden Sie im [IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS Konto, das Sie besitzen](#).

Es wird eine Aktualisierung der Benachrichtigungshäufigkeit empfohlen GuardDuty CloudWatch

In GuardDuty sind Melder mit einer CloudWatch Amazon-Benachrichtigungshäufigkeit konfiguriert, um nachfolgende Ereignisse eines Fundes zu melden. Dies beinhaltet das Senden von Benachrichtigungen an Detective.

Standardmäßig beträgt die Frequenz sechs Stunden. Das bedeutet, dass selbst wenn sich ein Befund viele Male wiederholt, die neuen Ereignisse erst bis zu sechs Stunden später in Detective widerspiegelt werden.

Um die Zeit zu reduzieren, die Detective benötigt, um diese Updates zu erhalten, empfehlen wir, dass das GuardDuty Administratorkonto die Einstellung seiner Melder auf 15 Minuten ändert.

Beachten Sie, dass eine Änderung der Konfiguration keine Auswirkungen auf die Nutzungskosten hat GuardDuty.

Informationen zur Einstellung der Benachrichtigungshäufigkeit finden Sie unter [Monitoring GuardDuty Findings with Amazon CloudWatch Events](#) im GuardDuty Amazon-Benutzerhandbuch.

Aktivieren von Amazon Detective

Sie können Detective über die Detective-Konsole, die Detective-API oder die AWS Command Line Interface aktivieren.

Sie können Detective in jeder Region nur einmal aktivieren. Wenn Sie bereits das Administratorkonto für ein Verhaltensdiagramm in der Region haben, können Sie Detective in dieser Region nicht erneut aktivieren.

Detective aktivieren (Konsole)

Sie können Amazon Detective über die AWS Management Console aktivieren.

So aktivieren Sie Detective (Konsole)

1. Melden Sie sich bei der an AWS Management Console. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie Erste Schritte.
3. Auf der Seite Amazon Detective aktivieren wird unter Administratorkonten ausrichten (empfohlen) die Empfehlung erläutert, die Administratorkonten zwischen Detective und Amazon abzustimmen GuardDuty und AWS Security Hub. Siehe [the section called "Empfohlene Ausrichtung mit und GuardDuty AWS Security Hub"](#).
4. Über die Schaltfläche „IAM-Richtlinie anhängen“ gelangen Sie direkt zur IAM-Konsole und öffnen die empfohlene Richtlinie. Sie haben die Möglichkeit, die empfohlene Richtlinie an den Principal anzuhängen, den Sie für Detective verwenden. Wenn Sie nicht über Berechtigungen für den Betrieb in der IAM-Konsole verfügen, können Sie im Bereich Erforderliche Berechtigungen die Richtlinie Amazon-Ressourcenname (ARN) kopieren, um sie Ihrem IAM-Administrator zur Verfügung zu stellen. Sie können die Richtlinie in Ihrem Namen anhängen.

Vergewissern Sie sich, dass die erforderliche IAM-Richtlinie vorhanden ist.

5. Im Abschnitt Tags hinzufügen können Sie dem Verhaltensdiagramm Tags hinzufügen.

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.

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

6. Wählen Sie Amazon Detective aktivieren.
7. Nachdem Sie Detective aktiviert haben, können Sie Mitgliedskonten zu Ihrem Verhaltensdiagramm einladen.

Um zur Kontoverwaltungsseite zu gelangen, wählen Sie Mitglieder jetzt hinzufügen. Informationen zum Einladen von Mitgliedskonten finden Sie unter [the section called "Mitgliedskonten zu einem Verhaltensdiagramm einladen"](#).

Detective aktivieren (Detective API, AWS CLI)

Sie können Amazon Detective über die Detective API oder die AWS Command Line Interface aktivieren.

Um Detective zu aktivieren (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [CreateGraph](#).
- AWS CLI: Führen Sie in der Befehlszeile den Befehl [create-graph](#) aus.

```
aws detective create-graph --tags '{"tagName": "tagValue"}
```

Der folgende Befehl aktiviert Detective und setzt den Wert des Department-Tags auf Security.

```
aws detective create-graph --tags '{"Department": "Security"}
```

Detective regionsübergreifend aktivieren (Python-Skript aktiviert GitHub)

Detective stellt ein Open-Source-Skript zur Verfügung GitHub , das Folgendes tut:

- Aktiviert Detective für ein Administratorkonto in einer bestimmten Liste von Regionen

- Fügt jedem der resultierenden Verhaltensdiagramme eine bereitgestellte Liste von Mitgliedskonten hinzu
- Sendet Einladungs-E-Mails an die Mitgliedskonten
- Nimmt die Einladungen für die Mitgliedskonten automatisch an

Hinweise zur Konfiguration und Verwendung der GitHub Skripts finden Sie unter [the section called “Amazon Detective Python-Skripte”](#).

Überprüfen, ob Daten extrahiert werden

Nachdem Sie Detective aktiviert haben, beginnt es, Daten aus Ihrem AWS Konto aufzunehmen und in Ihr Verhaltensdiagramm zu extrahieren.

Bei der ersten Extraktion stehen die Daten normalerweise innerhalb von 24 Stunden im Verhaltensdiagramm zur Verfügung.

Eine Möglichkeit, um zu überprüfen, ob Detective Daten extrahiert, besteht darin, beispielsweise Werte auf der Detective Such-Seite zu suchen.

So überprüfen Sie beispielsweise Werte auf der Suchseite

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Klicken Sie im Navigationsbereich auf Suchen.
3. Wählen Sie im Menü Typ auswählen einen Elementtyp aus.

Beispiele aus Ihren Daten enthalten einen Beispielsatz von Identifikatoren des ausgewählten Typs, die in Ihren Verhaltensdiagramm Daten enthalten sind.

Wenn Sie Beispielwerte sehen können, wissen Sie, dass Daten aufgenommen und in Ihr Verhaltensdiagramm extrahiert werden.

Konzepte und Terminologie von Amazon Detective

Die folgenden Begriffe und Konzepte sind für ein Verständnis der Funktionsweise von Amazon Detective wichtig.

Administratorkonto

AWS-Konto Derjenige, der ein Verhaltensdiagramm besitzt und das Verhaltensdiagramm zur Untersuchung verwendet.

Das Administratorkonto lädt Mitgliedskonten ein, ihre Daten zum Verhaltensdiagramm beizutragen. Weitere Informationen finden Sie unter [the section called “Mitgliedskonten zu einem Verhaltensdiagramm einladen”](#).

Für das Diagramm zum Organisationsverhalten ist das Administratorkonto das Detective-Administratorkonto, das das Verwaltungskonto der Organisation festlegt. Weitere Informationen finden Sie unter [the section called “Festlegen des Detective-Administratorkontos”](#). Das Detective Administrator-Konto kann jedes Organisationskonto als Mitgliedskonto im Verhaltensdiagramm der Organisation aktivieren. Weitere Informationen finden Sie unter [the section called “Mitgliedskonten von Organisationen verwalten”](#).

Administratorkonten können auch die Datennutzung für das Verhaltensdiagramm anzeigen und Mitgliedskonten aus dem Verhaltensdiagramm entfernen.

Organisation autonomer Systeme (ASO)

Die betitelte Organisation, der ein autonomes System zugewiesen ist. Dieses autonome System ist ein heterogenes Netzwerk oder eine Gruppe von Netzwerken, die ähnliche Routing-Logik und Richtlinien verwenden.

Verhaltensdiagramm

Ein verknüpfter Datensatz, der aus eingehenden Quelldaten generiert wird und mit einem oder mehreren AWS-Konten verknüpft ist.

Jedes Verhaltensdiagramm verwendet dieselbe Struktur von Erkenntnissen, Entitäten und Beziehungen.

Delegiertes Administratorkonto (AWS Organizations)

In Organizations kann das delegierte Administratorkonto für einen Dienst die Nutzung eines Dienstes für die Organisation verwalten.

In Detective ist das Detective-Administratorkonto auch das delegierte Administratorkonto, es sei denn, das Detective-Administratorkonto ist das Verwaltungskonto der Organisation. Das Verwaltungskonto der Organisation darf kein delegierter Administrator sein.

In Detective ist Selbstdelegation erlaubt. Das Verwaltungskonto einer Organisation kann sein eigenes Konto an den delegierten Administrator von Detective delegieren, aber dies würde nur im Bereich von Detective registriert oder gespeichert, nicht im Bereich von Organisationen.

Administratorkonto für Detective

Das Konto, das vom Verwaltungskonto der Organisation als Administratorkonto für das Verhaltensdiagramm der Organisation in einer Region festgelegt wurde. Weitere Informationen finden Sie unter [the section called “Festlegen des Detective-Administratorkontos”](#).

Detective empfiehlt, dass das Verwaltungskonto der Organisation ein anderes Konto als sein Konto auswählt.

Wenn es sich bei dem Konto nicht um das Verwaltungskonto der Organisation handelt, ist das Detective-Administratorkonto auch das delegierte Administratorkonto für Detective in Organizations.

Quelldaten von Detective

Verarbeitete, strukturierte Versionen von Informationen aus den folgenden Arten von Feeds:

- Protokolle von AWS Diensten, wie AWS CloudTrail Logs und Amazon VPC Flow Logs
- GuardDuty Ergebnisse

Detective verwendet die Detective-Quelldaten, um das Verhaltensdiagramm zu füllen. Detective speichert auch Kopien der Detective-Quelldaten, um seine Analysen zu unterstützen.

Entität

Ein Element, das aus den aufgenommenen Daten extrahiert wurde.

Jede Entität hat einen Typ, der den Objekttyp identifiziert, den sie repräsentiert. Beispiele für Entitätstypen sind IP-Adressen, Amazon EC2 EC2-Instances und AWS Benutzer.

Entitäten können AWS Ressourcen sein, die Sie verwalten, oder externe IP-Adressen, die mit Ihren Ressourcen interagiert haben.

Für jede Entität werden die Quelldaten auch verwendet, um Entitätseigenschaften aufzufüllen. Eigenschaftswerte können direkt aus Quelldatensätzen extrahiert oder über mehrere Datensätze hinweg aggregiert werden.

Erkenntnis

Ein von Amazon festgestelltes Sicherheitsproblem GuardDuty.

Erkenntnisgruppe

Eine Sammlung verwandter Erkenntnisse, Entitäten und Beweise, die sich möglicherweise auf dasselbe Ereignis oder Sicherheitsproblem beziehen. Detective generiert Suchgruppen auf der Grundlage eines integrierten Modells für Machine Learning.

Detective Beweise

Detective identifiziert zusätzliche Beweise im Zusammenhang mit einer Befundgruppe auf der Grundlage von Daten in Ihrem Verhaltensdiagramm, die in den letzten 45 Tagen gesammelt wurden. Diese Evidenz wird als Erkenntnis mit dem Schweregrad Informativ dargestellt. Beweise liefern unterstützende Informationen, die auf eine ungewöhnliche Aktivität oder ein unbekanntes Verhalten hinweisen, das möglicherweise verdächtig ist, wenn es innerhalb einer Erkenntnisgruppe betrachtet wird. Ein Beispiel hierfür könnten neu beobachtete Geolocations oder API-Aufrufe sein, die innerhalb des Zeitraums einer Erkenntnis beobachtet wurden. Derzeit sind diese Erkenntnisse nur in Detective sichtbar und werden nicht an Security Hub gesendet.

Überblick finden

Eine einzelne Seite, die eine Übersicht der Informationen zu einer Erkenntnis enthält.

Eine Übersicht über die Erkenntnisse enthält die Liste der beteiligten Entitäten für die Erkenntnisse. Von der Liste aus können Sie zum Profil einer Entität wechseln.

Eine Erkenntnisübersicht enthält auch einen Detailbereich, der die Suchattribute enthält.

Entität mit hohem Volumen

Eine Entität, die während eines Zeitintervalls Verbindungen zu oder von einer großen Anzahl anderer Entitäten unterhält. Eine EC2-Instance kann beispielsweise Verbindungen von Millionen von IP-Adressen haben. Die Anzahl der Verbindungen überschreitet den Schwellenwert, den Detective verarbeiten kann.

Wenn die aktuelle Gültigkeitsdauer ein großes Zeitintervall enthält, benachrichtigt Detective den Benutzer.

Weitere Informationen finden Sie im Amazon Detective Benutzerhandbuch unter [Details für Entitäten mit hohem Volumen anzeigen](#).

Untersuchung

Der Prozess, bei dem verdächtige oder interessante Aktivitäten ausfindig gemacht, ihr Umfang bestimmt, die zugrunde liegende Quelle oder Ursache ermittelt und dann festgelegt wird, wie vorzugehen ist.

Mitgliedskonto

Und AWS-Konto dass ein Administratorkonto aufgefordert wurde, Daten zu einem Verhaltensdiagramm beizutragen. Im Diagramm zum Organisationsverhalten kann ein Mitgliedskonto ein Organisationskonto sein, das das Detective-Administratorkonto als Mitgliedskonto aktiviert hat.

Eingeladene Mitgliedskonten können auf die Einladung zum Verhaltensdiagramm antworten und ihr Konto aus dem Verhaltensdiagramm entfernen. Weitere Informationen finden Sie unter [the section called “Für Mitgliedskonten: Einladungen und Mitgliedschaften verwalten”](#).

Organisations-Konten können ihre Mitgliedschaft im Verhaltensdiagramm der Organisation nicht ändern.

Alle Mitgliedskonten können auch Nutzungsinformationen für ihr Konto in den Verhaltensdiagrammen einsehen, zu denen sie Daten beitragen.

Sie haben keinen anderen Zugriff auf das Verhaltensdiagramm.

Diagramm zum Verhalten der Organisation

Das Verhaltensdiagramm, das dem Detective-Administratorkonto gehört. Das Verwaltungskonto der Organisation bezeichnet das Detective-Administratorkonto. Weitere Informationen finden Sie unter [the section called “Festlegen des Detective-Administratorkontos”](#).

Im Diagramm zum Organisationsverhalten steuert das Detective-Administratorkonto, ob es sich bei einem Organisationskonto um ein Mitgliedskonto handelt. Ein Organisationskonto kann sich nicht selbst aus dem Verhaltensdiagramm der Organisation entfernen.

Das Detective-Administratorkonto kann auch andere Konten zum Verhaltensdiagramm der Organisation einladen.

Profil

Eine einzelne Seite, die eine Sammlung von Datenvisualisierungen im Zusammenhang mit Aktivitäten für eine Entität enthält.

Bei Ergebnissen können Analysten anhand von Profilen feststellen, ob die Erkenntnis wirklich besorgniserregend oder falsch positiv ist.

Profile bieten Informationen zur Unterstützung einer Untersuchung eines Befundes oder zur allgemeinen Suche nach verdächtigen Aktivitäten.

Profilbereich

Eine einzelne Visualisierung in einem Profil. Jeder Profilbereich soll dazu beitragen, eine oder mehrere spezifische Fragen zu beantworten, um einen Analysten bei einer Untersuchung zu unterstützen.

Profilbereiche können Schlüssel-Wert-Paare, Tabellen, Zeitleisten, Balkendiagramme oder Geolokalisierungsdiagramme enthalten.

Beziehung

Aktivität, die zwischen einzelnen Entitäten stattfindet. Beziehungen werden auch aus den eingehenden Quelldaten extrahiert.

Ähnlich wie eine Entität hat eine Beziehung einen Typ, der die Typen der beteiligten Entitäten und die Richtung der Verbindung identifiziert. Ein Beispiel für einen Beziehungstyp ist eine IP-Adresse, die eine Verbindung zu einer Amazon-EC2-Instance herstellt.

Bereichsname

Das Zeitfenster, das für den Umfang der in Profilen angezeigten Daten verwendet wird.

Die standardmäßige Gültigkeitsdauer für einen Befund gibt an, wann die verdächtige Aktivität zum ersten und letzten Mal beobachtet wurde.

Die standardmäßige Gültigkeitsdauer für ein Entitätsprofil entspricht den letzten 24 Stunden.

Daten in einem Verhaltensdiagramm

In Amazon Detective führen Sie Untersuchungen anhand von Daten aus einem Verhaltensdiagramm von Detective durch.

Ein Verhaltensdiagramm ist ein verknüpfter Datensatz, der aus den Detective-Quelldaten generiert wird und von einem oder mehreren Amazon Web Services (AWS)-Konten aufgenommen wurde.

Das Verhaltensdiagramm verwendet die Quelldaten, um Folgendes zu erreichen:

- Verschaffen Sie sich ein Gesamtbild Ihrer Systeme, Benutzer und der Interaktionen zwischen ihnen im Laufe der Zeit
- Führen Sie detailliertere Analysen bestimmter Aktivitäten durch, um Fragen zu beantworten, die sich bei der Durchführung von Untersuchungen ergeben
- Korrelieren Sie Sammlungen von Erkenntnissen, Entitäten und Beweisen, die sich möglicherweise auf dasselbe Ereignis oder Sicherheitsproblem beziehen.

Beachten Sie, dass die gesamte Extraktion, Modellierung und Analyse von Verhaltensdiagrammdaten im Kontext jedes einzelnen Verhaltensdiagramms erfolgt.

Informationen darüber, wie ein Administratorkonto die Mitgliedskonten in einem Verhaltensdiagramm verwaltet, finden Sie unter [Konten verwalten](#).

Inhalt

- [Wie Amazon Detective Quelldaten verwendet, um ein Verhaltensdiagramm zu füllen](#)
- [Trainingszeit für neue Verhaltensdiagramme](#)
- [Überblick über die Datenstruktur des Verhaltensdiagramms](#)
- [In einem Verhaltensdiagramm verwendete Quelldaten](#)

Wie Amazon Detective Quelldaten verwendet, um ein Verhaltensdiagramm zu füllen

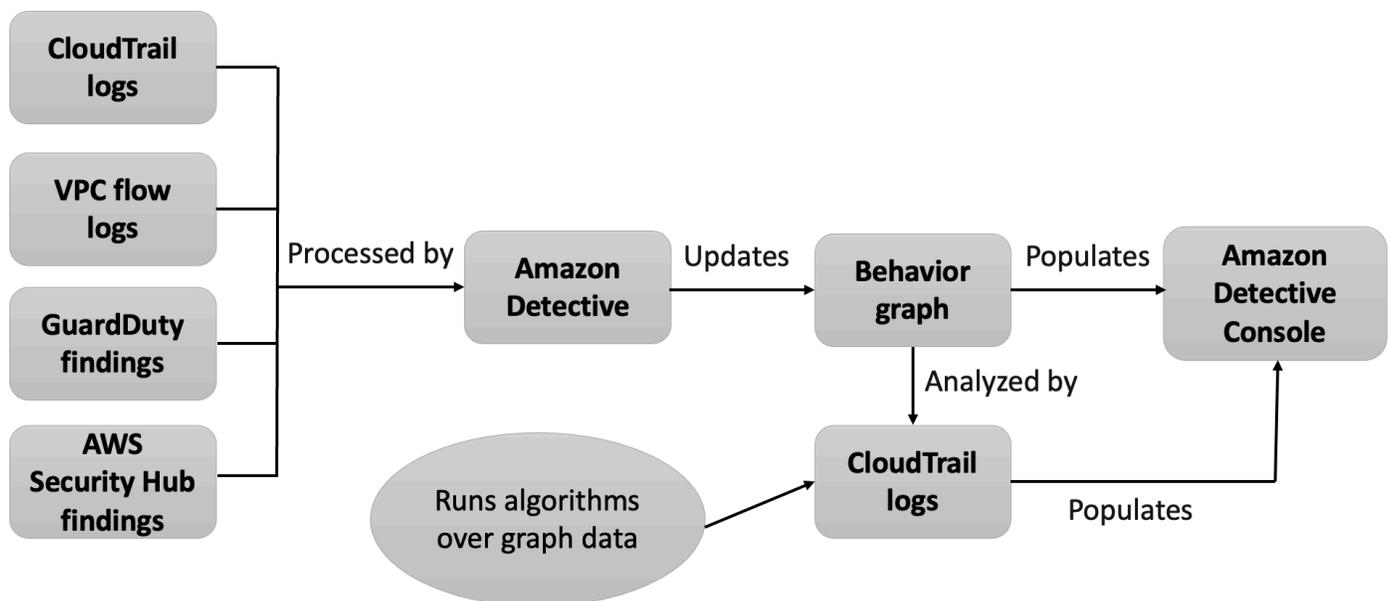
Um die Rohdaten für Untersuchungen bereitzustellen, führt Detective Daten aus Ihrer gesamten AWS-Umgebung und darüber hinaus zusammen, darunter die folgenden:

- Protokolldaten, einschließlich Amazon Virtual Private Cloud (Amazon VPC) und AWS CloudTrail
- Ergebnisse von Amazon GuardDuty
- Ergebnisse von AWS Security Hub

Weitere Informationen zu den in einem Verhaltensdiagramm verwendeten Quelldaten finden Sie unter [In einem Verhaltensdiagramm verwendete Quelldaten](#).

Wie Detective Quelldaten verarbeitet

Wenn neue Daten eintreffen, verwendet Detective eine Kombination aus Extraktion und Analyse, um das Verhaltensdiagramm zu füllen.



Detective-Extraktion

Die Extraktion basiert auf konfigurierten Zuordnungsregeln. Eine Zuordnungsregel besagt im Grunde: „Wann immer Sie diese Daten sehen, verwenden Sie sie auf diese spezielle Weise, um die Daten des Verhaltensdiagramms zu aktualisieren.“

Beispielsweise kann ein eingehender Detective-Quelldatensatz eine IP-Adresse enthalten. Ist dies der Fall, verwendet Detective die Informationen in diesem Datensatz, um eine neue IP-Adressentität zu erstellen oder eine bestehende IP-Adressentität zu aktualisieren.

Detective-Analysen

Bei Analysen handelt es sich um komplexere Algorithmen, die die Daten analysieren, um Einblicke in Aktivitäten zu gewinnen, die mit Entitäten verknüpft sind.

Eine Art von Detective-Analyse analysiert beispielsweise, wie oft Aktivitäten auftreten, indem Algorithmen ausgeführt werden. Bei Entitäten, die API-Aufrufe tätigen, sucht der Algorithmus nach API-Aufrufen, die die Entität normalerweise nicht verwendet. Der Algorithmus sucht auch nach einem starken Anstieg der Anzahl von API-Aufrufen.

Analytische Erkenntnisse unterstützen Untersuchungen, indem sie Antworten auf wichtige Analystenfragen liefern. Sie werden häufig verwendet, um Profilbereiche mit Ergebnissen und Entitätsprofilen zu füllen.

Trainingszeit für neue Verhaltensdiagramme

Eine Möglichkeit, eine Erkenntnis zu untersuchen, besteht darin, die Aktivität während des Untersuchungszeitraums mit Aktivitäten zu vergleichen, die vor der Entdeckung der Erkenntnis stattgefunden haben. Bei Aktivitäten, die noch nie zuvor beobachtet wurden, ist die Wahrscheinlichkeit höher, dass sie verdächtig sind.

In einigen Profilbereichen von Amazon Detective werden Aktivitäten hervorgehoben, die in der Zeit vor dem Befund nicht beobachtet wurden. In mehreren Profilbereichen wird auch ein Basiswert angezeigt, der die durchschnittliche Aktivität in den 45 Tagen vor dem Untersuchungszeitraum anzeigt. Die Gültigkeitsdauer ist die Zusammenfassung der Aktivitäten einer Entität im Zeitverlauf.

Je mehr Daten in Ihr Verhaltensdiagramm extrahiert werden, desto genauer kann sich Detective ein Bild davon machen, welche Aktivitäten in Ihrem Unternehmen normal und welche ungewöhnlich sind.

Um dieses Bild zu erstellen, benötigt Detective jedoch Zugriff auf Daten von mindestens zwei Wochen. Der Reifegrad der Detective-Analyse nimmt auch mit der Anzahl der Konten im Verhaltensdiagramm zu.

Die ersten zwei Wochen nach der Aktivierung von Detective gelten als Trainingszeit. Während dieses Zeitraums wird in Profilbereichen, in denen Aktivitäten im Umfang und in der Zeit mit früheren Aktivitäten verglichen werden, die Meldung angezeigt, dass sich Detective in einer Trainingsphase befindet.

Während der Testphase empfiehlt Detective, dass Sie dem Verhaltensdiagramm so viele Mitgliedskonten wie möglich hinzufügen. Dadurch verfügt Detective über einen größeren Datenpool, der es ermöglicht, ein genaueres Bild der normalen Aktivitäten in Ihrem Unternehmen zu erstellen.

Überblick über die Datenstruktur des Verhaltensdiagramms

Die Datenstruktur des Verhaltensdiagramms definiert die Struktur der extrahierten und analysierten Daten. Sie definiert auch, wie die Quelldaten dem Verhaltensdiagramm zugeordnet werden.

Arten von Elementen in der Datenstruktur des Verhaltensdiagramms

Die Datenstruktur des Verhaltensdiagramms besteht aus den folgenden Informationselementen.

Entität

Eine Entität stellt ein Element dar, das aus den Detective-Quelldaten extrahiert wurde.

Jede Entität hat einen Typ, der den Objekttyp identifiziert, den sie repräsentiert. Beispiele für Entitätstypen sind IP-Adressen, Amazon EC2 EC2-Instances und AWS Benutzer.

Für jede Entität werden die Quelldaten auch verwendet, um Entitätseigenschaften aufzufüllen. Eigenschaftswerte können direkt aus Quelldatensätzen extrahiert oder über mehrere Datensätze hinweg aggregiert werden.

Einige Eigenschaften bestehen aus einem einzelnen skalaren oder aggregierten Wert. Für eine EC2-Instance verfolgt Detective beispielsweise den Instance-Typ und die Gesamtzahl der verarbeiteten Byte.

In den Eigenschaften von Zeitreihen wird die Aktivität im Laufe der Zeit verfolgt. Für eine EC2-Instance verfolgt Detective beispielsweise im Laufe der Zeit die eindeutigen Ports, die sie verwendet hat.

Beziehungen

Eine Beziehung stellt eine Aktivität dar, die zwischen einzelnen Entitäten stattfindet. Beziehungen werden auch aus den Detective-Quelldaten extrahiert.

Ähnlich wie eine Entität hat eine Beziehung einen Typ, der die Typen der beteiligten Entitäten und die Richtung der Verbindung identifiziert. Ein Beispiel für einen Beziehungstyp sind IP-Adressen, die eine Verbindung zu EC2-Instances herstellen.

Für jede einzelne Beziehung, z. B. eine bestimmte IP-Adresse, die eine Verbindung zu einer bestimmten Instanz herstellt, verfolgt Detective die Ereignisse im Laufe der Zeit.

Arten von Entitäten in der Datenstruktur des Verhaltensdiagramms

Die Datenstruktur des Verhaltensdiagramms besteht aus Entitäts- und Beziehungstypen, die Folgendes bewirken:

- Verfolgen der verwendeten Server, IP-Adressen und Benutzeragenten
- Verfolgen Sie die verwendeten AWS Benutzer, Rollen und Konten
- Verfolgen Sie die Netzwerkverbindungen und Autorisierungen, die in Ihrer AWS -Umgebung auftreten

Die Datenstruktur des Verhaltensdiagramms enthält die folgenden Entitätstypen.

AWS Konto

AWS Konten, die in den Detective-Quelldaten vorhanden sind.

Für jedes Konto beantwortet Detective mehrere Fragen:

- Welche API-Aufrufe hat das Konto verwendet?
- Welche Benutzeragenten hat das Konto verwendet?
- Welche autonomen Systemorganisationen (ASOs) hat das Konto verwendet?
- An welchen geografischen Standorten war das Konto aktiv?

AWS Rolle

AWS Rollen, die in den Detective-Quelldaten vorhanden sind.

Für jede Rolle beantwortet Detective mehrere Fragen:

- Welche API-Aufrufe hat die Rolle verwendet?
- Welche Benutzeragenten hat die Rolle verwendet?
- Welches ASOs hat die Rolle verwendet?
- An welchen geografischen Standorten war die Rolle aktiv?
- Welche Ressourcen haben diese Rolle übernommen?
- Welche Rollen hat diese Rolle übernommen?

- In welchen Rollensitzungen wurde diese Rolle behandelt?

AWS Benutzer

AWS Benutzer, die in den Detective-Quelldaten vorhanden sind.

Für jeden Benutzer beantwortet Detective mehrere Fragen:

- Welche API-Aufrufe hat der Benutzer verwendet?
- Welche Benutzeragenten hat der Benutzer verwendet?
- An welchen geografischen Standorten war der Benutzer aktiv?
- Welche Rollen hat dieser Benutzer übernommen?
- An welchen Rollensitzungen war dieser Benutzer beteiligt?

Verbundbenutzer

Instances eines Verbundbenutzers. Beispiele für Verbundbenutzer sind unter anderem:

- Eine Identität, die sich mit Security Assertion Markup Language (SAML) anmeldet
- Eine Identität, die sich mithilfe eines Web-Identitätsverbunds anmeldet

Detective beantwortet für jeden Verbundbenutzer die folgenden Fragen:

- Mit welchem Identitätsanbieter hat sich der Verbundbenutzer authentifiziert?
- Was war die Zielgruppe des Verbundbenutzers? Die Zielgruppe identifiziert die Anwendung, die das Web-Identitätstoken des Verbundbenutzers angefordert hat.
- An welchen geografischen Standorten war der Verbundbenutzer aktiv?
- Welche Benutzeragenten hat der Verbundbenutzer verwendet?
- Welches ASOs hat der Verbundbenutzer verwendet?
- Welche Rollen hat dieser Verbundbenutzer übernommen?
- An welchen Rollensitzungen war dieser Verbundbenutzer beteiligt?

EC2-Instance

EC2-Instances, die in den Detective-Quelldaten vorhanden sind.

Für EC2-Instances beantwortet Detective mehrere Fragen:

- Welche IP-Adressen haben mit der Instance kommuniziert?
- Welche Ports wurden für die Kommunikation mit der Instance verwendet?
- Welches Datenvolumen wurde an und von der Instance gesendet?

- Welche VPC enthält die Instance?
- Welche API-Aufrufe hat die EC2-Instance verwendet?
- Welche Benutzeragenten hat die EC2-Instance verwendet?
- Welches ASOs hat die EC2-Instance verwendet?
- An welchen geografischen Standorten war die EC2-Instance aktiv?
- Welche Rollen hat die EC2-Instance übernommen?

Rollensitzungen

Instances einer Ressource, die eine Rolle übernimmt. Jede Rollensitzung wird durch die Rollen-ID und einen Sitzungsnamen identifiziert.

Für jede Rolle beantwortet Detective mehrere Fragen:

- Welche Ressourcen waren an dieser Rollensitzung beteiligt? Mit anderen Worten, welche Rolle wurde übernommen und welche Ressource hat diese Rolle übernommen?

Beachten Sie, dass Detective bei kontoübergreifender Rollenübernahme die Ressource nicht identifizieren kann, die die Rolle übernommen hat.

- Welche API-Aufrufe wurden in der Rollensitzung verwendet?
- Welche Benutzeragenten wurden in der Rollensitzung verwendet?
- Welches ASOs wurde in der Rollensitzung verwendet?
- An welchen geografischen Standorten war die Rollensitzung aktiv?
- Welcher Benutzer oder welche Rolle hat diese Rollensitzung gestartet?
- Welche Rollensitzungen wurden von dieser Rollensitzung aus gestartet?

Erkenntnis

Von Amazon aufgedeckte Ergebnisse, die in GuardDuty die Quelldaten von Detective eingespeist werden.

Für jeden Befund verfolgt Detective den Befundtyp, den Ursprung und das Zeitfenster für die Erkenntnisaktivität.

Außerdem werden Informationen gespeichert, die für die Erkenntnis spezifisch sind, z. B. Rollen oder IP-Adressen, die an der erkannten Aktivität beteiligt sind.

IP-Adresse

IP-Adressen, die in den Detective-Quelldaten vorhanden sind.

Für jede IP-Adresse beantwortet Detective mehrere Fragen:

- Welche API-Aufrufe hat die Adresse verwendet?
- Welche Ports hat die Adresse verwendet?
- Welche Benutzer und Benutzeragenten haben die IP-Adresse verwendet?
- An welchen geografischen Standorten war die IP-Adresse aktiv?
- Welchen EC2-Instances wurde diese IP-Adresse zugewiesen und mit welchen wurde kommuniziert?

S3-Bucket

S3-Buckets, die sich in den Detective-Quelldaten befinden.

Für jeden S3-Bucket beantwortet Detective die folgenden Fragen:

- Welche Prinzipale haben mit dem S3-Bucket interagiert?
- Welche API-Aufrufe wurden an den S3-Bucket getätigt?
- Von welchen geografischen Standorten aus haben Prinzipale API-Aufrufe an den S3-Bucket getätigt?
- Welche Benutzeragenten wurden verwendet, um mit dem S3-Bucket zu interagieren?
- Welche ASOs wurden für die Interaktion mit dem S3-Bucket verwendet?

Sie können einen S3-Bucket löschen und dann einen neuen Bucket mit demselben Namen erstellen. Da Detective den S3-Bucket-Namen verwendet, um den S3-Bucket zu identifizieren, behandelt er diese als eine einzelne S3-Bucket-Entität. Im Entitätsprofil ist die Erstellungszeit die erste Erstellungszeit. Die Löschzeit ist die letzte Löschzeit.

Um alle Erstellungs- und Löschereignisse anzuzeigen, legen Sie den Gültigkeitszeitraum so fest, dass er mit der Erstellungszeit beginnt und mit der Löschzeit endet. Zeigen Sie im Profilbereich für das gesamte API-Aufrufvolumen die Aktivitätsdetails für den Gültigkeitszeitraum an. Filtern Sie die API-Methoden zur Anzeige von Create- und Delete-Methoden. Siehe [the section called "Gesamtes API-Aufrufvolumen"](#).

Benutzer-Agent

Benutzeragenten, die in den Detective-Quelldaten vorhanden sind.

Für jeden Benutzeragenten beantwortet Detective Fragen wie die folgenden:

- Welche API-Aufrufe hat der Benutzeragent verwendet?
- Welche Benutzer und Rollen haben den Benutzeragenten verwendet?

- Welche IP-Adressen haben den Benutzeragenten verwendet?

EKS-Cluster

EKS-Cluster, die in den Detective-Quelldaten vorhanden sind.

Note

Um vollständige Details für diesen Entitätstyp anzuzeigen, muss die optionale EKS-Auditprotokoll-Datenquelle aktiviert sein. Weitere Informationen finden Sie unter [Optionale Datenquellen](#)

Für jeden EKS-Cluster beantwortet Detective Fragen wie die folgenden:

- Welche Kubernetes-API-Aufrufe wurden in diesem Cluster ausgeführt?
- Welche Kubernetes-Benutzer und Service-Konten (Subjekte) sind in diesem Cluster aktiv?
- Welche Container wurden in diesem Cluster gestartet?
- Welche Images werden verwendet, um Container in diesem Cluster zu starten?

Kubernetes-Pod

Kubernetes-Pods, die in den Detective-Quelldaten vorhanden sind.

Note

Um vollständige Details für diesen Entitätstyp anzuzeigen, muss die optionale EKS-Auditprotokoll-Datenquelle aktiviert sein. Weitere Informationen finden Sie unter [Optionale Datenquellen](#)

Für jeden Pod beantwortet Detective Fragen wie die folgenden:

- Welche Container-Images in diesem Pod sind in meinen Konten üblich?
- Welche Aktivität wurde auf diesen Pod gerichtet?
- Welche Container laufen in diesem Pod?
- Sind Registrierungen von Containern in diesem Pod in meinen Konten üblich?
- Welche anderen Container werden in den anderen Pods der Workload ausgeführt?
- Gibt es ungewöhnliche Container in diesem Pod, die sich nicht in den anderen Pods des Workloads befinden?

Container-Image

Container-Images, die in den Detective-Quelldaten vorhanden sind.

Note

Um vollständige Details für diesen Entitätstyp anzuzeigen, muss die optionale EKS-Auditprotokoll-Datenquelle aktiviert sein. Weitere Informationen finden Sie unter [Optionale Datenquellen](#)

Für jedes Container-Image beantwortet Detective Fragen wie die folgenden:

- Welche anderen Images in meiner Umgebung nutzen dasselbe Repository oder dieselbe Registry wie dieses Image?
- Wie viele Kopien dieses Images werden in meiner Umgebung ausgeführt?

Kubernetes Betreff

Kubernetes-Themen, die in den Detective-Quelldaten enthalten sind. Ein Kubernetes-Betreff ist ein Benutzer- oder Dienstkonto.

Note

Um vollständige Details für diesen Entitätstyp anzuzeigen, muss die optionale EKS-Auditprotokoll-Datenquelle aktiviert sein. Weitere Informationen finden Sie unter [Optionale Datenquellen](#)

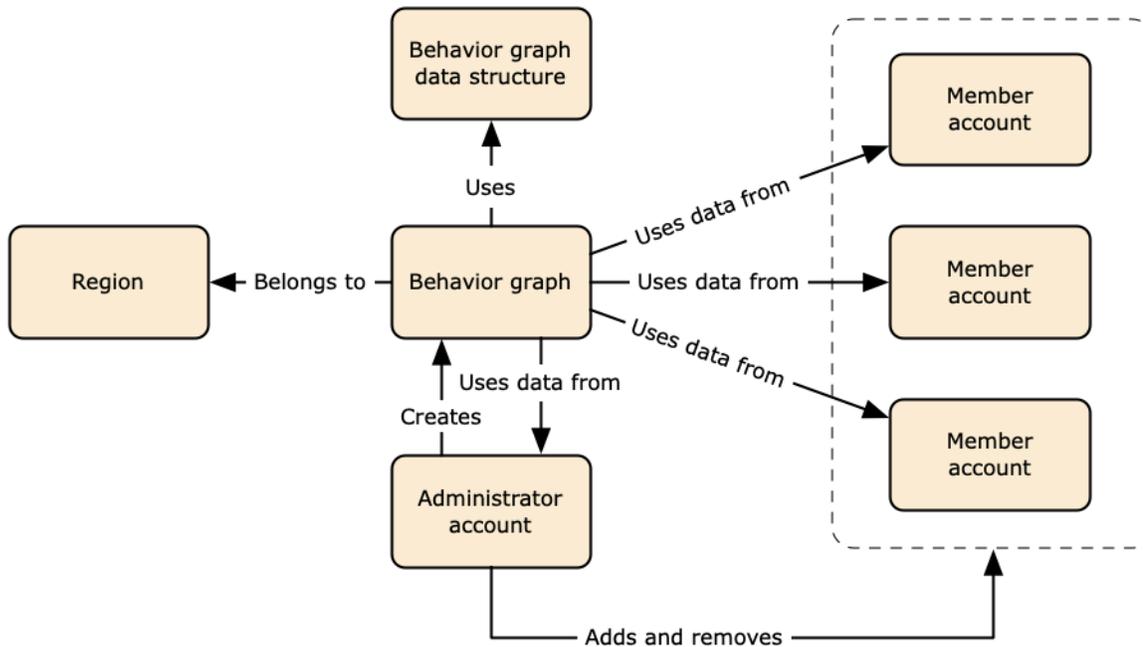
Zu jedem Thema beantwortet Detective Fragen wie die folgenden:

- Welche IAM-Prinzipale haben sich für diesen Betreff authentifiziert?
- Welche Erkenntnisse sind mit diesem Thema verbunden?
- Welche IP-Adressen verwendet die Testperson?

In einem Verhaltensdiagramm verwendete Quelldaten

Um ein Verhaltensdiagramm aufzufüllen, verwendet Amazon Detective Quelldaten aus dem Administratorkonto und den Mitgliedskonten des Verhaltensdiagramms.

Mit Detective können Sie auf historische Ereignisdaten von bis zu einem Jahr zugreifen. Diese Daten sind über eine Reihe von Visualisierungen verfügbar, die Veränderungen in Art und Umfang der Aktivitäten in einem ausgewählten Zeitfenster zeigen. Detective verknüpft diese Änderungen mit GuardDuty Ergebnissen.



Einzelheiten zur Datenstruktur des Verhaltensdiagramms finden Sie unter [Überblick über die Datenstruktur des Verhaltensdiagramms](#) im Detective-Benutzerhandbuch.

Arten von Kerndatenquellen in Detective

Detective nimmt Daten aus diesen Arten von AWS Protokollen auf:

- AWS CloudTrail Logs
- Amazon Virtual Private Cloud (Amazon VPC)-Datendurchflussprotokolle
 - Nimmt sowohl IPv4- als auch IPv6-Datensätze auf, jedoch keine MAC-Datensätze, die von Elastic Fabric Adapters erstellt wurden.
 - Nimmt Protokolldatensätze auf, wenn sich der log-status Feldwert im Status befindet. OK Weitere Informationen finden Sie unter [Flow-Protokolldatensätze](#) im Amazon VPC-Benutzerhandbuch.
 - Nimmt Flow-Logs auf, die von Amazon Elastic Compute Cloud-Instances erstellt wurden, die nur in diesen VPCs ausgeführt werden. Es werden keine anderen Ressourcen wie NAT-Gateways, RDS-Instances oder Fargate-Cluster verwendet.
 - Nimmt sowohl akzeptierten als auch abgelehnten Datenverkehr auf.

- Für Konten, für die registriert ist GuardDuty, nimmt Detective auch Ergebnisse auf. GuardDuty

Detective verarbeitet CloudTrail und protokolliert VPC-Flow-Ereignisse mithilfe unabhängiger und duplizierter Streams von CloudTrail VPC-Flow-Logs. Diese Prozesse wirken sich nicht auf Ihre vorhandenen Konfigurationen und Ihre VPC-Flow-Log-Konfigurationen aus CloudTrail und verwenden diese auch nicht. Sie wirken sich auch nicht auf die Leistung dieser Dienste aus und erhöhen auch nicht Ihre Kosten.

Arten optionaler Datenquellen in Detective

Detective bietet zusätzlich zu den drei Datenquellen, die im Detective-Kernpaket angeboten werden, optionale Quellpakete an (das Kernpaket umfasst AWS CloudTrail Protokolle, VPC Flow-Protokolle und GuardDuty Ergebnisse). Ein optionales Datenquellenpaket kann für ein Verhaltensdiagramm jederzeit gestartet oder gestoppt werden.

Detective bietet eine kostenlose 30-Tage-Testversion für alle Kern- und optionalen Quellpakete pro Region.

Note

Detective bewahrt alle von jedem Datenquellenpaket empfangenen Daten bis zu 1 Jahr lang auf.

Derzeit sind die folgenden optionalen Quellpakete verfügbar:

- EKS-Auditprotokolle

Mit diesem optionalen Datenquellenpaket kann Detective detaillierte Informationen zu EKS-Clustern in Ihrer Umgebung aufnehmen und diese Daten Ihrem Verhaltensdiagramm hinzufügen. Detective korreliert Benutzeraktivitäten mit CloudTrail AWS-Management-Ereignissen und Netzwerkaktivitäten mit Amazon VPC Flow Logs, ohne dass Sie diese Protokolle manuell aktivieren oder speichern müssen. Details dazu finden Sie unter [Amazon EKS-Auditprotokolle für Detective](#).

- AWS Ergebnisse zur Sicherheit

Mit diesem optionalen Datenquellenpaket kann Detective Daten aus Security Hub aufnehmen und diese Daten Ihrem Verhaltensdiagramm hinzufügen. Details dazu finden Sie unter [AWS Ergebnisse zur Sicherheit](#).

Starten oder Stoppen einer optionalen Datenquelle:

1. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Klicken Sie im Navigationsbereich unter Einstellungen auf Allgemein.
3. Wählen Sie unter Optionale Quellpakete die Option Update aus. Wählen Sie dann die Datenquelle aus, die Sie aktivieren oder deaktivieren möchten, ein Feld für eine bereits aktivierte Datenquelle und wählen Sie Aktualisieren, um zu ändern, welche Datenquellenpakete aktiviert sind.

Note

Wenn Sie eine optionale Datenquelle beenden und dann neu starten, sehen Sie eine Lücke in den in einigen Entitätsprofilen angezeigten Daten. Diese Lücke wird in der Konsolenanzeige angezeigt und steht für den Zeitraum, in dem die Datenquelle gestoppt wurde. Wenn eine Datenquelle neu gestartet wird, nimmt Detective keine Daten rückwirkend auf.

Amazon EKS-Auditprotokolle für Detective

Amazon EKS Audit Logs sind ein optionales Datenquellenpaket, das Ihrem Detective-Verhaltensdiagramm hinzugefügt werden kann. Sie können die verfügbaren optionalen Quellpakete und deren Status in Ihrem Konto auf der Einstellungsseite in der Konsole oder über die Detective-API einsehen.

Für diese Datenquelle steht eine kostenlose 30-Tage-Testversion zur Verfügung. Weitere Informationen hierzu finden Sie unter [Kostenlose Testversion für optionale Datenquellen](#).

Durch die Aktivierung von Amazon EKS-Auditprotokollen kann Detective Ihrem Verhaltensdiagramm detaillierte Informationen über mit Amazon EKS erstellte Ressourcen hinzufügen. Diese Datenquelle erweitert die bereitgestellten Informationen zu den folgenden Entitätstypen: EKS-Cluster, Kubernetes-Pod, Container-Image und Kubernetes-Sujet.

Wenn Sie EKS-Audit-Logs als Datenquelle in Amazon aktiviert haben, können GuardDuty Sie außerdem Details zu den Ergebnissen von Kubernetes einsehen. GuardDuty Weitere Informationen zur Aktivierung dieser Datenquelle GuardDuty finden Sie unter [Kubernetes-Schutz in Amazon](#).
GuardDuty

Note

Diese Datenquelle ist standardmäßig für neue Verhaltensdiagramme aktiviert, die nach dem 26. Juli 2022 erstellt wurden. Für Verhaltensdiagramme, die vor dem 26. Juli 2022 erstellt wurden, muss sie manuell aktiviert werden.

Hinzufügen oder Entfernen von Amazon EKS-Auditprotokollen als optionale Datenquelle:

1. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Klicken Sie im Navigationsbereich unter Einstellungen auf Allgemein.
3. Wählen Sie unter Quellpakete die Option EKS-Auditprotokolle aus, um diese Datenquelle zu aktivieren. Wenn sie bereits aktiviert ist, wählen Sie sie erneut aus, um die Aufnahme von EKS-Auditprotokollen in Ihr Verhaltensdiagramm zu beenden.

AWS Ergebnisse zur Sicherheit

AWS security findings ist ein optionales Datenquellenpaket, das zu Ihrem Detective-Verhaltensdiagramm hinzugefügt werden kann.

Sie können die verfügbaren optionalen Quellpakete und deren Status in Ihrem Konto auf der Einstellungsseite in der Konsole oder über die Detective-API einsehen.

Für diese Datenquelle steht eine kostenlose 30-Tage-Testversion zur Verfügung. Weitere Informationen hierzu finden Sie unter [Kostenlose Testversion für optionale Datenquellen](#).

Durch die Aktivierung von AWS Sicherheitserkenntnissen kann Detective die Erkenntnisse von Security Hub, die von Security Hub aus Upstream-Services aggregiert wurden, in einem Standarderkenntnisformat, dem AWS Security Format (ASFF), verwenden, wodurch zeitaufwändige Datenkonvertierungen überflüssig werden. Anschließend werden aufgenommene Funde über Produkte hinweg korreliert, um die wichtigsten zu priorisieren.

AWS Sicherheitsergebnisse als optionale Datenquelle hinzufügen oder entfernen:

Note

Die Datenquelle für AWS Sicherheitsergebnisse ist standardmäßig für neue Verhaltensdiagramme aktiviert, die nach dem 16. Mai 2023 erstellt wurden. Für

Verhaltensdiagramme, die vor dem 16. Mai 2023 erstellt wurden, muss sie manuell aktiviert werden.

1. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Klicken Sie im Navigationsbereich unter Einstellungen auf Allgemein.
3. Wählen Sie unter Quellpakete die Option AWS Sicherheitsergebnisse aus, um diese Datenquelle zu aktivieren. Wenn sie bereits aktiviert ist, wählen Sie sie erneut aus, um die Aufnahme von Erkenntnissen des AWS Security Finding Format (ASFF) in Ihr Verhaltensdiagramm zu beenden.

Derzeit unterstützte Erkenntnisse

Detective nimmt alle ASFF-Ergebnisse in Security Hub von Diensten auf, die Amazon gehören oder AWS

- Eine Liste der unterstützten Service-Integrationen finden Sie unter [Verfügbare AWS-Serviceintegrationen](#) im AWS Security Hub Benutzerhandbuch.
- Eine Liste der unterstützten Ressourcen finden Sie unter [Ressourcen](#) im AWS Security Hub - Benutzerhandbuch.
- AWS Serviceergebnisse, bei denen der Compliance-Status nicht auf festgelegt ist, FAILED und regionsübergreifende aggregierte Ergebnisse werden nicht aufgenommen.

Wie Detective Quelldaten aufnimmt und speichert

Wenn Detective aktiviert ist, beginnt es mit der Aufnahme von Quelldaten aus dem Administratorkonto für Verhaltensdiagramme. Sobald Mitgliedskonten zum Verhaltensdiagramm hinzugefügt werden, beginnt Detective auch, die Daten aus diesen Mitgliedskonten zu verwenden.

Die Quelldaten von Detective bestehen aus strukturierten und verarbeiteten Versionen der ursprünglichen Feeds. Um Detective Analytics zu unterstützen, speichert Detective Kopien der Detective-Quelldaten.

Der Detective-Ingest-Prozess speist Daten in Amazon Simple Storage Service (Amazon S3)-Buckets im Detective-Quelldatenspeicher. Sobald neue Quelldaten eintreffen, nehmen andere Detective-Komponenten die Daten auf und starten die Extraktions- und Analyseprozesse. Weitere Informationen finden Sie unter [So verwendet Detective Quelldaten, um ein Verhaltensdiagramm zu füllen](#) im Detective-Benutzerhandbuch.

Wie Detective das Datenvolumenkontingent für Verhaltensdiagramme durchsetzt

Detective hat strenge Kontingente für das Datenvolumen, das in jedem Verhaltensdiagramm zulässig ist. Das Datenvolumen ist die Datenmenge pro Tag, die in das Detective-Verhaltensdiagramm fließt.

Detective setzt diese Kontingente durch, wenn ein Administratorkonto Detective aktiviert und wenn ein Mitgliedskonto eine Einladung annimmt, zu einem Verhaltensdiagramm beizutragen.

- Wenn das Datenvolumen für ein Administratorkonto 10 TB pro Tag übersteigt, kann das Administratorkonto Detective nicht aktivieren.
- Wenn das hinzugefügte Datenvolumen von einem Mitgliedskonto dazu führen würde, dass das Verhaltensdiagramm 10 TB pro Tag überschreitet, kann das Mitgliedskonto nicht aktiviert werden.

Das Datenvolumen für ein Verhaltensdiagramm kann im Laufe der Zeit auch auf natürliche Weise zunehmen. Detective überprüft täglich das Datenvolumen des Verhaltensdiagramms, um sicherzustellen, dass das Kontingent nicht überschritten wird.

Wenn sich das Datenvolumen des Verhaltensdiagramms dem Kontingent nähert, zeigt Detective eine Warnmeldung auf der Konsole an. Um zu verhindern, dass das Kontingent überschritten wird, können Sie Mitgliedskonten entfernen.

Wenn das Datenvolumen des Verhaltensdiagramms 10 TB pro Tag überschreitet, können Sie dem Verhaltensdiagramm kein neues Mitgliedskonto hinzufügen.

Wenn das Datenvolumen des Verhaltensdiagramms 15 TB pro Tag überschreitet, beendet Detective die Aufnahme von Daten in das Verhaltensdiagramm. Das Kontingent von 15 TB pro Tag spiegelt sowohl das normale Datenvolumen als auch Spitzenwerte beim Datenvolumen wider. Wenn dieses Kontingent erreicht ist, werden keine neuen Daten in das Verhaltensdiagramm aufgenommen, aber vorhandene Daten werden nicht entfernt. Sie können diese historischen Daten weiterhin für Untersuchungen verwenden. In der Konsole wird eine Meldung angezeigt, die darauf hinweist, dass die Datenaufnahme für das Verhaltensdiagramm unterbrochen wurde.

Wenn die Datenaufnahme unterbrochen wurde, müssen Sie damit arbeiten, sie wieder AWS Support zu aktivieren. Versuchen Sie nach Möglichkeit, vor der Kontaktaufnahme Mitgliedskonten zu entfernen AWS Support, um das Datenvolumen unter das Kontingent zu bringen. Dadurch ist es einfacher, die Datenaufnahme für das Verhaltensdiagramm wieder zu aktivieren.

Wie Amazon Detective für Ermittlungen verwendet wird

Amazon Detective macht es Ihnen leicht, die Ursache von Sicherheitserkenntnissen oder verdächtigen Aktivitäten zu analysieren, zu untersuchen und schnell zu identifizieren. Wenn Sie Detective noch nicht kennen, finden Sie weitere Informationen unter [Was ist Amazon Detective?](#) und [Konzepte und Terminologie von Amazon Detective](#).

Themen

- [Detective Untersuchung](#)
- [Ermittlungsphasen und Ausgangspunkte](#)
- [Ablauf der Amazon Detective Investigation](#)

Detective Untersuchung

Sie können Amazon Detective Investigation verwenden, um IAM-Benutzer und IAM-Rollen anhand von Kompromissindikatoren zu untersuchen, anhand derer Sie feststellen können, ob eine Ressource an einem Sicherheitsvorfall beteiligt ist. 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. Mit Detective Investigations können Sie die Effizienz maximieren, sich auf Sicherheitsbedrohungen konzentrieren und die Reaktionsfähigkeit auf Vorfälle verbessern.

Detective Investigation verwendet Modelle für maschinelles Lernen und Bedrohungsinformationen, um Ressourcen in Ihrer AWS Umgebung automatisch zu analysieren und potenzielle Sicherheitsvorfälle zu identifizieren. Damit können Sie die Automatisierung, die auf dem Verhaltensdiagramm von Detective basiert, proaktiv, effektiv und effizient nutzen, um die Sicherheitsabläufe zu verbessern. Mit Detective Investigations können Sie Angriffstaktiken, unmögliche Reisen, markierte IP-Adressen und das Auffinden von Gruppen untersuchen. Es führt erste Schritte zur Sicherheitsuntersuchung durch und generiert einen Bericht, in dem die von Detective identifizierten Risiken hervorgehoben werden, damit Sie Sicherheitsereignisse besser verstehen und auf potenzielle Vorfälle reagieren können.

Durchführung einer Detective Untersuchung

Verwenden Sie Untersuchung durchführen, um Ressourcen wie IAM-Benutzer und IAM-Rollen zu analysieren und einen Untersuchungsbericht zu erstellen. Der generierte Bericht beschreibt ein ungewöhnliches Verhalten, das auf eine mögliche Gefährdung hindeutet.

Console

Gehen Sie wie folgt vor, um eine Detective Investigation von der Seite Investigations aus mithilfe der Amazon Detective-Konsole durchzuführen.

1. Melden Sie sich bei der AWS Management Console an. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
 2. Wählen Sie im Navigationsbereich die Option Untersuchungen.
 3. Wählen Sie auf der Seite Ermittlungen oben rechts die Option Untersuchung ausführen aus.
 4. Im Bereich Ressource auswählen haben Sie drei Möglichkeiten, eine Untersuchung durchzuführen. Sie können wählen, ob Sie die Untersuchung für eine von Detective empfohlene Ressource durchführen möchten. Sie können die Untersuchung für eine bestimmte Ressource durchführen. Sie können eine Ressource auch über die Such-Seite in Detective untersuchen.
1. Choose a recommended resource— Detective empfiehlt Ressourcen auf der Grundlage seiner Aktivitäten in Ermittlungs- und Findungsgruppen. Um die Untersuchung für eine von Detective empfohlene Ressource durchzuführen, wählen Sie in der Tabelle Empfohlene Ressourcen eine zu untersuchende Ressource aus.

Die Tabelle der empfohlenen Ressourcen bietet die folgenden Informationen:

- Ressourcen-ARN — Der Amazon-Ressourcenname (ARN) der AWS Ressource.
- Grund für die Untersuchung: Zeigt die wichtigsten Gründe für die Untersuchung der Ressource an. Mögliche Gründe, aus denen Detective empfiehlt, eine Ressource zu untersuchen, sind:
 - Wenn bei einer Ressource in den letzten 24 Stunden ein schwerwiegender Fehler festgestellt wurde.
 - Wenn eine Ressource Teil einer in den letzten 7 Tagen beobachteten Erkenntnisgruppe war. Mithilfe von Detective-Erkennnisgruppen können Sie mehrere Aktivitäten untersuchen, da sie sich auf ein potenzielles Sicherheitsereignis beziehen. Weitere Details finden Sie unter [the section called “Gruppen finden”](#).

- Wenn eine Ressource Gegenstand einer Erkenntnis in den letzten 7 Tagen war.
 - Letzte Erkenntnis: Die aktuellen Erkenntnisse stehen ganz oben auf der Liste.
 - Ressourcentyp: Identifiziert den Ressourcentyp. Zum Beispiel ein AWS Benutzer oder eine AWS Rolle.
2. Specify an AWS role or user with an ARN— Sie können eine AWS Rolle oder einen AWS Benutzer auswählen und eine Untersuchung für die jeweilige Ressource durchführen.

Gehen Sie wie folgt vor, um einen bestimmten Ressourcentyp zu untersuchen.

- a. Wählen Sie in der Dropdownliste Ressourcentyp auswählen die AWS Rolle oder den AWS Benutzer aus.
 - b. Geben Sie den Ressourcen-ARN der IAM-Ressource ein. Weitere Informationen zu Ressourcen-ARNs finden Sie unter [Amazon Resource Names \(ARNs\)](#) im IAM-Benutzerhandbuch.
3. Find a resource to investigate from the Search page— Sie können alle Ihre IAM-Ressourcen auf der Detective Search-Seite durchsuchen.

Gehen Sie wie folgt vor, um eine Ressource von der Suchseite aus zu untersuchen.

- a. Klicken Sie im Navigationsbereich auf Suchen.
 - b. Suchen Sie auf der Suchseite nach einer IAM-Ressource.
 - c. Navigieren Sie zur Profilsseite der Ressource und führen Sie von dort aus die Untersuchung durch.
5. Wählen Sie im Abschnitt Dauer des Untersuchungsumfangs den Zeitraum für den Umfang der Untersuchung aus, um die Aktivität der ausgewählten Ressource zu bewerten. Sie können ein Startdatum und eine Startzeit sowie ein Enddatum und eine Endzeit im UTC-Format auswählen. Das gewählte Zeitfenster für den Geltungsbereich kann zwischen mindestens 3 Stunden und maximal 30 Tagen liegen.
6. Wählen Sie Untersuchung ausführen aus.

API

Verwenden Sie den [StartInvestigation](#) Betrieb der Detective-API, um eine Untersuchung programmgesteuert durchzuführen. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [start-investigation](#) aus.

Verwenden Sie in Ihrer Anforderung diese Parameter, um eine Untersuchung in Detective durchzuführen:

- `GraphArn`: Geben Sie den Amazon-Ressourcennamen (ARN) des Verhaltensdiagramms an.
- `EntityArn`: Geben Sie den eindeutigen Amazon-Ressourcennamen (ARN) des IAM-Benutzers und der IAM-Rolle an.
- `ScopeStartTime`: Geben Sie optional das Datum und die Uhrzeit an, ab dem die Untersuchung beginnen soll. Der Wert ist eine UTC-Zeichenfolge im ISO8601-Format. Beispiel: `2021-08-18T16:35:56.284Z`
- `ScopeEndTime`: Geben Sie optional das Datum und die Uhrzeit an, ab dem die Untersuchung enden soll. Der Wert ist eine UTC-Zeichenfolge im ISO8601-Format. Beispiel: `2021-08-18T16:35:56.284Z`

Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
aws detective start-investigation \  
--graph-arn arn:aws:detective:us-  
east-1:123456789123:graph:fdac8011456e4e6182facb26dfceade0  
--entity-arn arn:aws:iam::123456789123:role/rolename --scope-start-  
time 2023-09-27T20:00:00.00Z  
--scope-end-time 2023-09-28T22:00:00.00Z
```

Sie können eine Untersuchung auch über die folgenden Seiten in Detective durchführen:

- Die Profilsseite eines IAM-Benutzers oder einer IAM-Rolle in Detective.
- Bereich zur grafischen Darstellung einer Erkenntnisgruppe.
- Spalte „Aktionen“ einer beteiligten Ressource.
- IAM-Benutzer oder IAM-Rolle auf einer Erkenntnisseite.

Sobald Detective die Untersuchung für eine Ressource durchgeführt hat, wird ein Untersuchungsbericht generiert. Um auf den Bericht zuzugreifen, wechseln Sie im Navigationsbereich zu Untersuchungen.

Überprüfen von Untersuchungsberichten

Mit Untersuchungsberichten können Sie die generierten Berichte für Untersuchungen überprüfen, die Sie zuvor in Detective ausgeführt haben.

So überprüfen Sie Untersuchungsberichte

1. Melden Sie sich bei der AWS Management Console an. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich die Option Untersuchungen.

Beachten Sie die folgenden Merkmale aus einem Untersuchungsbericht.

- **ID** – Die generierte Kennung des Untersuchungsberichts. Sie können diese ID wählen, um eine Übersicht des Untersuchungsberichts mit den Einzelheiten der Untersuchung zu lesen.
- **Status** – Jeder Untersuchung ist ein Status zugeordnet, der auf dem Abschlussstatus der Untersuchung basiert. Die Statuswerte können In Bearbeitung, Erfolgreich oder Fehlgeschlagen lauten.
- **Schweregrad** – Jeder Untersuchung wird ein Schweregrad zugewiesen. Der Detective weist der Erkenntnis automatisch einen Schweregrad zu.

Ein Schweregrad steht für die Disposition, wie sie bei der Untersuchung einer einzelnen Ressource zu einem bestimmten Zeitpunkt analysiert wurde. Ein im Rahmen einer Untersuchung gemeldeter Schweregrad impliziert nicht die Wichtigkeit oder Bedeutung, die eine betroffene Ressource für Ihr Unternehmen haben könnte, und gibt auch keinen Hinweis darauf.

Der Schweregrad einer Untersuchung kann als Kritisch, Hoch, Mittel, Niedrig oder Informativ vom höchsten bis zum geringsten Schweregrad angegeben werden.

Untersuchungen, denen der Schweregrad „Kritisch“ oder „Hoch“ zugewiesen wurde, sollten für eine weitere Überprüfung priorisiert werden, da es sich bei ihnen mit größerer Wahrscheinlichkeit um von Detective identifizierte Sicherheitsprobleme mit schwerwiegenden Auswirkungen handelt.

- **Entität** – Die Spalte Entität enthält Details zu den spezifischen Entitäten, die bei der Untersuchung entdeckt wurden. Bei einigen Entitäten handelt es sich um AWS Konten, z. B. Benutzer und Rollen.
- **Status** – Die Spalte Erstellungsdatum enthält Angaben zu Datum und Uhrzeit der ersten Erstellung des Untersuchungsberichts.

Einen Detective Investigations-Bericht verstehen

Ein Detective Investigations-Bericht enthält eine Zusammenfassung des ungewöhnlichen Verhaltens oder der böswilligen Aktivität, die auf eine Beeinträchtigung hindeuten. Er listet auch die Empfehlungen auf, die Detective zur Minderung des Sicherheitsrisikos vorschlägt.

Admin report summary Info High

We observed anomalous behavior for the role from [redacted] indicating potential compromise. The role invoked CloudTrail management actions mapped to Impact MITRE tactic(s). The role was also involved in Findings that map to the MITRE tactic(s) Discovery, as well as other tactic(s). The role was also involved in 10 findings, 1 finding group, 170 impossible travels, 3 new geolocations, and 5 new user agents.

Scope time 05/25/2023 13:00 UTC - 05/31/2023 19:00 UTC	Indicators of compromise 5 Tactics 0 Flagged IP 170 Impossible travel 1 Finding group	Recommendation Based on our investigation, we recommend you take action to mitigate what we've found on AWS role Admin. Please review Security Best Practices in IAM to secure your AWS resource.
---	---	--

So zeigen Sie einen Untersuchungsbericht für eine bestimmte Ermittlungsnummer an.

1. Melden Sie sich bei der AWS Management Console an. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich die Option Untersuchungen.
3. Wählen Sie in der Tabelle Berichte eine Untersuchungs-ID aus.

Detective generiert den Bericht für den ausgewählten Gültigkeitszeitraum und den ausgewählten Benutzer. Der Bericht enthält einen Abschnitt mit Kompromissindikatoren, der Einzelheiten zu einem oder mehreren der unten aufgeführten Kompromissindikatoren enthält. Wählen Sie bei der Überprüfung der einzelnen Kompromissindikatoren optional ein Element aus, das Sie genauer untersuchen und dessen Einzelheiten Sie überprüfen möchten.

- Taktiken. Techniken und Verfahren – Identifiziert Taktiken, Techniken und Verfahren (TTPs), die bei einem potenziellen Sicherheitsereignis zum Einsatz kommen. Das MITRE ATT&CK-Framework wird verwendet, um die TTPs zu verstehen. Die Taktiken basieren auf der [MITRE](#) ATT&CK-Matrix für Unternehmen.
- Mit Threat Intelligence markierte IP-Adressen – Verdächtige IP-Adressen werden gekennzeichnet und auf der Grundlage von Detective Threat Intelligence als kritische oder schwerwiegende Bedrohungen identifiziert.

- **Unmögliche Reise** – Erkennt und identifiziert ungewöhnliche und unmögliche Benutzeraktivitäten für ein Konto. Dieser Indikator listet beispielsweise eine drastische Änderung zwischen Quell- und Zielort eines Benutzers innerhalb einer kurzen Zeitspanne auf.
- **Verwandte Erkenntnisgruppe** – Zeigt mehrere Aktivitäten an, die sich auf ein potenzielles Sicherheitsereignis beziehen. Detective verwendet Diagrammanalysetechniken, um Beziehungen zwischen Erkenntnissen und Entitäten abzuleiten und sie zu einer Erkenntnisgruppe zusammenzufassen.
- **Verwandte Erkenntnisse** – Verwandte Aktivitäten im Zusammenhang mit einem potenziellen Sicherheitsereignis. Listet alle unterschiedlichen Kategorien von Beweisen auf, die mit der Ressource oder der Erkenntnisgruppe in Verbindung stehen.
- **Neue Geolocations** – Identifiziert neue Geolocations, die entweder auf Ressourcen- oder Kontoebene verwendet werden. Dieser Indikator listet beispielsweise eine beobachtete Geolocation auf, bei der es sich aufgrund früherer Benutzeraktivitäten um einen seltenen oder ungenutzten Standort handelt.
- **Neue Benutzeragenten** – Identifiziert neue Benutzeragenten, die entweder auf Ressourcen- oder Kontoebene verwendet werden.
- **Neue ASOs** – Identifiziert neue Autonomous System Organizations (ASOs), die entweder auf Ressourcen- oder Kontoebene verwendet werden. Dieser Indikator listet beispielsweise eine neue Organisation auf, die als ASO zugewiesen wurde.

Übersicht des Untersuchungsberichts

In der Übersicht der Untersuchungen werden für den ausgewählten Zeitraum ungewöhnliche Indikatoren hervorgehoben, die besondere Aufmerksamkeit erfordern. Anhand der Übersicht können Sie schneller die Ursache potenzieller Sicherheitsprobleme identifizieren, Muster erkennen und die Ressourcen verstehen, die von Sicherheitsereignissen betroffen sind.

In der Übersicht des Untersuchungsberichts finden Sie die folgenden Details.

Untersuchungsübersicht

Im Bereich Übersicht finden Sie eine Visualisierung von IPs mit Aktivität mit hohem Schweregrad, die Ihnen mehr Informationen über den Weg eines Angriffs geben kann.

Detective hebt ungewöhnliche Aktivitäten bei der Untersuchung hervor, z. B. die unmögliche Reise des IAM-Benutzers von einer Quelle zu einem weit entfernten Ziel.

Detective ordnet die Ermittlungen den Taktiken, Techniken und Verfahren (TTPs) zu, die bei einem potenziellen Sicherheitsereignis verwendet werden. Das MITRE ATT&CK-Framework wird verwendet, um die TTPs zu verstehen. Die Taktiken basieren auf der [MITRE](#) ATT&CK-Matrix für Unternehmen.

Untersuchungsindikatoren

Anhand der Informationen im Bereich Indikatoren können Sie feststellen, ob eine AWS -Ressource an ungewöhnlichen Aktivitäten beteiligt ist, die auf böses Verhalten und dessen Auswirkungen hinweisen könnten. 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.

Untersuchungsbericht herunterladen

Sie können den Detective Investigations-Bericht im JSON-Format herunterladen, um ihn weiter zu analysieren, oder ihn in Ihrer bevorzugten Speicherlösung wie einem Amazon S3 S3-Bucket speichern.

So laden Sie einen Untersuchungsbericht aus der Tabelle Berichte herunter.

1. Melden Sie sich bei der AWS Management Console an. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich die Option Untersuchungen.
3. Wählen Sie in der Tabelle Berichte eine Untersuchung aus und klicken Sie auf Herunterladen.

So laden Sie einen Untersuchungsbericht von der Übersichtsseite herunter.

1. Melden Sie sich bei der AWS Management Console an. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich die Option Untersuchungen.
3. Wählen Sie in der Tabelle Berichte eine Untersuchung aus.
4. Wählen Sie auf der Seite mit der Übersicht der Untersuchungen die Option Herunterladen aus.

Archivieren eines Untersuchungsberichts

Wenn Sie Ihre Untersuchung in Amazon Detective abgeschlossen haben, können Sie den Untersuchungsbericht Archivieren. Eine archivierte Untersuchung zeigt an, dass Sie die Überprüfung der Untersuchung abgeschlossen haben.

Sie können eine Untersuchung nur archivieren oder deren Archivierung aufheben, wenn Sie Detective Administrator sind. Detective speichert Ihre archivierten Untersuchungen 90 Tage lang.

So archivieren Sie einen Untersuchungsbericht aus der Tabelle Berichte.

1. Melden Sie sich bei der AWS Management Console an. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich die Option Untersuchungen.
3. Wählen Sie in der Tabelle Berichte eine Untersuchung aus und klicken Sie dann auf Archivieren.

So archivieren Sie einen Untersuchungsbericht von der Übersichtsseite aus.

1. Melden Sie sich bei der AWS Management Console an. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich die Option Untersuchungen.
3. Wählen Sie in der Tabelle Berichte eine Untersuchung aus.
4. Wählen Sie auf der Seite mit der Übersicht der Untersuchungen die Option Archivieren aus.

Ermittlungsphasen und Ausgangspunkte

Amazon Detective bietet Tools zur Unterstützung des gesamten Untersuchungsprozesses. Eine Untersuchung in Detective kann mit einer Erkenntnis, einer Erkenntnisgruppe oder einer Entität beginnen.

Phasen der Untersuchung

Jeder Untersuchungsprozess umfasst die folgenden Phasen:

Triage

Der Untersuchungsprozess beginnt, wenn Sie über einen Verdacht auf böswillige Aktivitäten oder Aktivitäten mit hohem Risiko informiert werden. Sie sind beispielsweise damit beauftragt,

Ergebnisse oder Warnungen zu untersuchen, die von Diensten wie Amazon GuardDuty und Amazon Inspector aufgedeckt wurden.

In der Triage-Phase stellen Sie fest, ob es sich bei der Aktivität Ihrer Meinung nach um eine echt positive Aktivität (echte böswillige Aktivität) oder um eine falsch positive Aktivität (keine böswillige oder risikoreiche Aktivität) handelt. Detective-Profile unterstützen den Triage-Prozess, indem sie Einblicke in die Aktivitäten der beteiligten Entität bieten.

In wirklich positiven Fällen fahren Sie mit der nächsten Phase fort.

Umfang

Während der Scoping-Phase ermitteln Analysten das Ausmaß der böswilligen oder risikoreichen Aktivität und die zugrunde liegende Ursache.

Beim Scoping werden die folgenden Arten von Fragen beantwortet:

- Welche Systeme und Benutzer wurden kompromittiert?
- Wo hat der Angriff seinen Ursprung?
- Wie lange dauert der Angriff schon an?
- Gibt es noch andere verwandte Aktivitäten, die aufgedeckt werden müssen? Wenn ein Angreifer beispielsweise Daten aus Ihrem System extrahiert, wie hat er diese erhalten?

Detective-Visualisierungen können Ihnen helfen, andere beteiligte oder betroffene Entitäten zu identifizieren.

Antwort

Der letzte Schritt besteht darin, auf den Angriff zu reagieren, um ihn zu stoppen, den Schaden zu minimieren und zu verhindern, dass ein ähnlicher Angriff erneut stattfindet.

Ausgangspunkte für eine Detective Untersuchung

Jede Untersuchung in Detective hat einen wesentlichen Ausgangspunkt. Möglicherweise wird Ihnen ein Amazon GuardDuty oder AWS Security Hub ein Fundstück zugewiesen, das Sie untersuchen möchten. Oder Sie haben Bedenken wegen ungewöhnlicher Aktivitäten für eine bestimmte IP-Adresse.

Zu den typischen Ausgangspunkten für eine Untersuchung gehören Ergebnisse, die von Detective-Quelldaten entdeckt wurden, GuardDuty und Entitäten, die aus diesen extrahiert wurden.

Festgestellte Ergebnisse von GuardDuty

GuardDuty verwendet Ihre Protokolldaten, um vermutete böswillige oder risikoreiche Aktivitäten aufzudecken. Detective stellt Ressourcen zur Verfügung, mit denen Sie diese Erkenntnisse untersuchen können.

Für jede Erkenntnis stellt Detective die zugehörigen Erkenntnisdetails zur Verfügung. Detective zeigt auch die Entitäten, wie IP-Adressen und AWS Konten, die mit dem Ergebnis verbunden sind.

Anschließend können Sie die Aktivitäten der beteiligten Entitäten untersuchen, um festzustellen, ob die anhand der Erkenntnis festgestellte Aktivität tatsächlich Anlass zur Sorge gibt.

Weitere Informationen finden Sie unter [the section called “Überblick über Erkenntnisse”](#).

AWS Von Security Hub aggregierte Sicherheitsergebnisse

AWS Security Hub fasst die Sicherheitsergebnisse verschiedener Anbieter von Erkenntnissen an einem einzigen Ort zusammen und bietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus in. AWS Security Hub eliminiert die Komplexität der Bewältigung großer Mengen an Erkenntnissen von mehreren Anbietern. Dadurch wird der Aufwand für die Verwaltung und Verbesserung der Sicherheit all Ihrer AWS Konten, Ressourcen und Workloads reduziert. Detective stellt Ressourcen zur Verfügung, mit denen Sie diese Erkenntnisse untersuchen können.

Für jede Erkenntnis stellt Detective die zugehörigen Erkenntnisdetails zur Verfügung. Detective zeigt auch die Entitäten, wie IP-Adressen und AWS Konten, die mit dem Ergebnis verbunden sind.

Weitere Informationen finden Sie unter [the section called “Überblick über Erkenntnisse”](#).

Aus Detective-Quelldaten extrahierte Entitäten

Aus den aufgenommenen Detective-Quelldaten extrahiert Detective Entitäten wie IP-Adressen und AWS -Benutzer. Sie können eine davon als Ausgangspunkt für Ermittlungen verwenden.

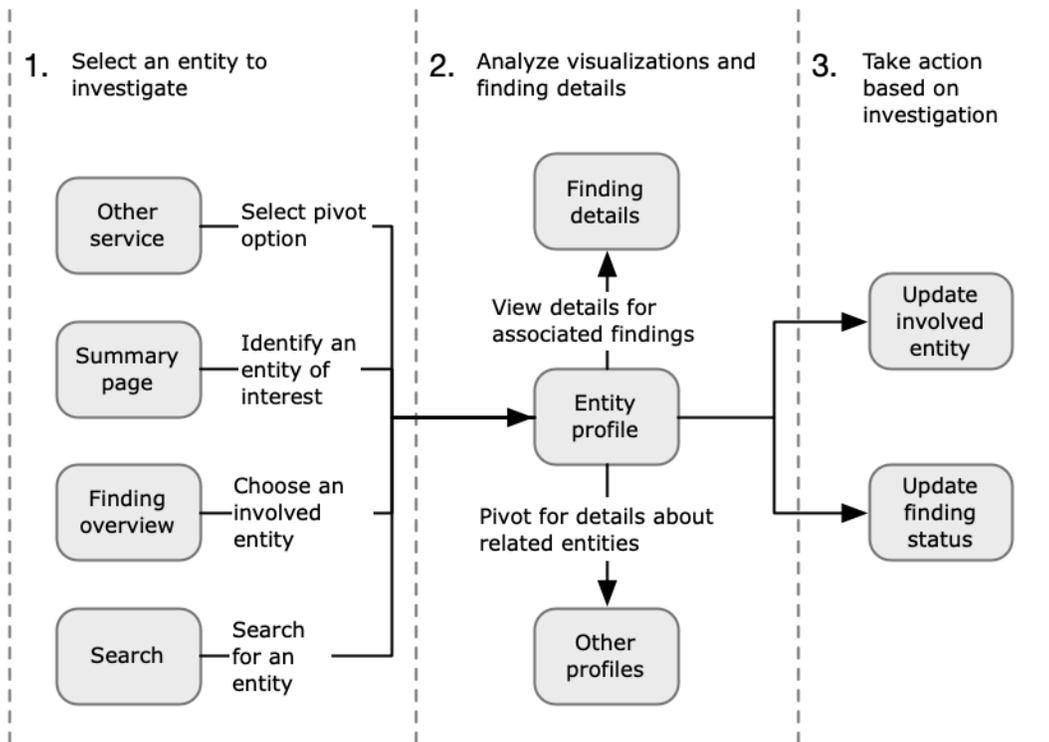
Detective stellt allgemeine Informationen über die Entität bereit, z. B. die IP-Adresse oder den Benutzernamen. Es enthält auch Details zum Aktivitätsverlauf. Detective kann beispielsweise melden, mit welchen anderen IP-Adressen eine Entität eine Verbindung hergestellt hat, mit welchen eine Verbindung hergestellt wurde oder welche sie verwendet hat.

Weitere Informationen finden Sie unter [Entitäten analysieren](#).

Ablauf der Amazon Detective Investigation

Sie können Amazon Detective verwenden, um eine Entität wie eine EC2-Instanz oder einen AWS Benutzer zu untersuchen. Sie können auch Sicherheitserkenntnisse untersuchen.

Auf einer höheren Ebene zeigt das folgende Bild den Ablauf einer Detective Untersuchung.



Schritt 1: Wählen Sie die zu untersuchende Entität

Bei der Analyse eines Ergebnisses in können sich Analysten dafür entscheiden GuardDuty, eine zugehörige Entität in Detective zu untersuchen. Siehe [the section called “Von einer anderen Konsole aus wechseln”](#).

Wenn Sie die Entität auswählen, gelangen Sie zum Entitätsprofil in Detective.

Schritt 2: Analysieren von Visualisierungen auf Profilen

Jedes Entitätsprofil enthält eine Reihe von Visualisierungen, die aus dem Verhaltensdiagramm generiert werden. Das Verhaltensdiagramm wird aus den Protokolldateien und anderen Daten erstellt, die in Detective eingespeist werden.

Die Visualisierungen zeigen Aktivitäten, die sich auf eine Entität beziehen. Sie verwenden diese Visualisierungen, um Fragen zu beantworten und festzustellen, ob die Entitätsaktivität ungewöhnlich ist. Siehe [Entitäten analysieren](#).

Als Hilfestellung bei der Untersuchung können Sie die Detective-Anleitungen verwenden, die für jede Visualisierung bereitgestellt werden. Die Anleitung beschreibt die angezeigten Informationen, schlägt Fragen vor, die Sie stellen können, und schlägt auf der Grundlage der Antworten die nächsten Schritte vor. Siehe [the section called “Verwendung von Anleitungen durch den Profilbereich”](#).

Jedes Profil enthält eine Liste der zugehörigen Erkenntnisse. Sie können die Details zu einer Erkenntnis und die Erkenntnisübersicht anzeigen. Siehe [the section called “Erkenntnisse für eine Entität anzeigen”](#).

Von einem Entitätsprofil aus können Sie zu anderen Entitäten und Suchprofilen wechseln, um die Aktivitäten in Bezug auf verwandte Ressourcen genauer zu untersuchen.

Schritt 3: Maßnahmen ergreifen

Ergreifen Sie auf der Grundlage der Erkenntnisse Ihrer Untersuchung die entsprechenden Maßnahmen.

Bei einer falsch-positiven Erkenntnis können Sie diese archivieren. Von Detective aus können Sie GuardDuty Ergebnisse archivieren. Siehe [the section called “Archivierung eines GuardDuty Befundes”](#).

Andernfalls ergreifen Sie die entsprechenden Maßnahmen, um die Sicherheitsanfälligkeit zu beheben und den Schaden zu minimieren. Beispielsweise müssen Sie möglicherweise die Konfiguration einer Ressource aktualisieren.

Ergebnisse in Amazon Detective analysieren

Eine Erkenntnis ist ein Fall einer potenziell böswilligen Aktivität oder eines anderen Risikos, das erkannt wurde. Amazon GuardDuty - und AWS Sicherheitsergebnisse werden in Amazon Detective geladen, sodass Sie Detective verwenden können, um die Aktivitäten im Zusammenhang mit den beteiligten Entitäten zu untersuchen. GuardDuty Die Ergebnisse sind Teil des Detective-Kernpakets und werden standardmäßig aufgenommen. Alle anderen AWS Sicherheitsergebnisse, die von Security Hub aggregiert werden, werden als optionale Datenquelle aufgenommen. Weitere Informationen finden Sie unter [In einem Verhaltensdiagramm verwendete Quelldaten](#).

Eine Übersicht über die Erkenntnisse von Detective bietet detaillierte Informationen über die Erkenntnis. Außerdem wird eine Übersicht der beteiligten Entitäten mit Links zu den zugehörigen Entitätsprofilen angezeigt.

Wenn eine Erkenntnis mit einer größeren Aktivität korreliert, weist Detective Sie darauf hin, zur Erkenntnisgruppe zu gehen. Wir empfehlen, Erkenntnisgruppen zu verwenden, um Ihre Untersuchung fortzusetzen, da Sie anhand von Erkenntnisgruppen mehrere Aktivitäten untersuchen können, die sich auf ein potenzielles Sicherheitsereignis beziehen. Siehe [the section called “Gruppen finden”](#).

Inhalt

- [Analyse einer Ergebnisübersicht](#)
- [Erkenntnisgruppen analysieren](#)
- [Erkenntnisgruppenübersicht basierend auf generativer KI](#)

Analyse einer Ergebnisübersicht

Eine Übersicht über die Erkenntnisse von Detective bietet detaillierte Informationen über die Erkenntnis. Außerdem wird eine Übersicht der beteiligten Entitäten mit Links zu den zugehörigen Entitätsprofilen angezeigt.

Zeitbereich, der für die Erkenntnisübersicht verwendet wurden

Der Zeitbereich einer Erkenntnisübersicht wird auf das Zeitfenster für die Suche festgelegt. Das Zeitfenster für die Erkenntnisse gibt an, wann die Erkenntnisaktivität zum ersten und letzten Mal beobachtet wurde.

Erkenntnisdetails

Das Feld auf der rechten Seite enthält die Details zur Erkenntnis. Dies sind die Details, die vom Erkenntnisanbieter bereitgestellt wurden.

Anhand der Erkenntnisdetails können Sie den Befund auch archivieren. Siehe [the section called “Archivierung eines GuardDuty Befundes”](#).

Verbundene Entitäten

Die Erkenntnisübersicht enthält eine Liste der Entitäten, die an der Erkenntnis beteiligt waren. Für jede Entität enthält die Liste Übersichtsinformationen über die Entität. Diese Informationen spiegeln die Informationen im Profilbereich mit den Entitätsdetails des entsprechenden Entitätsprofils wider.

Sie können die Liste basierend auf dem Entitätstyp filtern. Sie können die Liste auch basierend auf Text in der Entität-ID filtern.

Um zum Profil einer Entität zu wechseln, wählen Sie Profil anzeigen. Wenn Sie zum Entitätsprofil wechseln, geschieht Folgendes:

- Die Gültigkeitsdauer ist auf das Zeitfenster für die Suche festgelegt.
- Im Bereich Zugeordnete Erkenntnisse für die Entität wird die Erkenntnis ausgewählt. Die Erkenntnisdetails werden weiterhin auf der rechten Seite des Entitätsprofils angezeigt.

Problembehandlung bei „Seite nicht gefunden“

Wenn Sie in Detective zu einer Entität oder einer Erkenntnis navigieren, wird möglicherweise die Fehlermeldung Seite nicht gefunden angezeigt.

Gehen Sie wie folgt vor, um dieses Problem zu lösen:

- Vergewissern Sie sich, dass die Entität oder die Erkenntnis zu einem Ihrer Mitgliedskonten gehört. Informationen zur Überprüfung von Mitgliedskonten finden Sie unter [Kontenliste anzeigen](#).
- Stellen Sie sicher, dass Ihr Administratorkonto mit GuardDuty und/oder Security Hub abgestimmt ist, damit Sie von diesen Diensten zu Detective wechseln können. Die Empfehlungen finden Sie unter [Empfohlene Ausrichtung mit GuardDuty und Security Hub](#).
- Vergewissern Sie sich, dass die Erkenntnis gewonnen wurde, nachdem das Mitgliedskonto Ihre Einladung angenommen hat.

- Stellen Sie sicher, dass das Detective-Verhaltensdiagramm Daten aus einem optionalen Datenquellenpaket aufnimmt. Weitere Informationen zu Quelldaten, die in Verhaltensdiagrammen von Detective verwendet werden, finden Sie unter [In einem Verhaltensdiagramm verwendete Quelldaten](#).
- Damit Detective Daten aus Security Hub aufnehmen und diese Daten Ihrem Verhaltensdiagramm hinzufügen kann, müssen Sie Detective for AWS Security Findings als Datenquellenpaket aktivieren. Weitere Informationen finden Sie unter [AWS Sicherheitsergebnisse](#).
- Wenn Sie in Detective zu einem Entitätsprofil navigieren oder nach einer Erkenntnisübersicht suchen, stellen Sie sicher, dass die URL das richtige Format hat. Einzelheiten zur Erstellung einer Profil-URL finden Sie unter [Navigation zu einem Entitätsprofil oder Übersichtssuche mithilfe einer URL](#).

Erkenntnisgruppen analysieren

Mithilfe von Amazon-Detective-Erkenntnisgruppen können Sie mehrere Aktivitäten untersuchen, da sie sich auf ein potenzielles Sicherheitsereignis beziehen. Mithilfe von Finding Groups können Sie die Ursache für GuardDuty Befunde mit hohem Schweregrad analysieren. Wenn ein Bedrohungsakteur versucht, Ihre AWS Umgebung zu kompromittieren, führt er in der Regel eine Abfolge von Aktionen durch, die zu mehreren Sicherheitsergebnissen und ungewöhnlichem Verhalten führen. Diese Aktionen sind häufig über mehrere Zeiträume und Entitäten verteilt. Wenn Sicherheitserkenntnisse isoliert untersucht werden, kann dies zu einer Fehlinterpretation ihrer Bedeutung und zu Schwierigkeiten bei der Suche nach der Ursache führen. Amazon Detective löst dieses Problem, indem es eine Diagrammanalysetechnik anwendet, die Beziehungen zwischen Erkenntnissen und Entitäten ableitet und diese gruppiert. Wir empfehlen, Erkenntnisgruppen als Ausgangspunkt für die Untersuchung der beteiligten Entitäten und Erkenntnisse zu verwenden.

Detective analysiert Daten aus Erkenntnissen und gruppiert sie mit anderen Erkenntnissen, die aufgrund der gemeinsamen genutzten Ressourcen wahrscheinlich verwandt sind. Beispielsweise sind Erkenntnisse in Zusammenhang mit Aktionen, die von denselben IAM-Rollensitzungen ausgeführt wurden oder von derselben IP-Adresse stammen, sehr wahrscheinlich Teil derselben zugrunde liegenden Aktivität. Es ist ratsam, Erkenntnisse und Beweise als Gruppe zu untersuchen, auch wenn die von Detective gemachten Assoziationen nicht miteinander zusammenhängen.

Neben den Erkenntnissen umfasst jede Gruppe auch Einrichtungen, die von den Erkenntnissen betroffen sind. Zu den Entitäten können externe Ressourcen AWS wie IP-Adressen oder Benutzeragenten gehören.

Note

Nach einem ersten GuardDuty Befund, der mit einem anderen Befund zusammenhängt, wird innerhalb von 48 Stunden die Ergebnisgruppe mit allen zugehörigen Ergebnissen und allen beteiligten Entitäten erstellt.

Grundlegendes zur Seite „Erkenntnisgruppen“

Auf der Seite „Erkenntnisgruppen“ werden alle von Amazon Detective anhand Ihres Verhaltensdiagramms gesammelten Erkenntnisgruppen aufgeführt. Beachten Sie beim Suchen von Gruppen die folgenden Attribute:

Schweregrad einer Gruppe

Jeder Ergebnisgruppe wird ein Schweregrad zugewiesen, der auf dem Schweregrad der zugehörigen Ergebnisse im ASFF (AWS Security Finding Format) basiert. Die Schweregradwerte der ASFF-Erkenntnisse lauten Kritisch, Hoch, Mittel, Niedrig oder Informativ, vom höchsten bis zum geringsten Schweregrad. Der Schweregrad einer Gruppierung entspricht der Erkenntnis mit dem höchsten Schweregrad unter den Erkenntnissen in dieser Gruppierung.

Gruppen, die aus Erkenntnissen mit kritischem oder hohem Schweregrad bestehen, die sich auf eine große Anzahl von Entitäten auswirken, sollten bei Untersuchungen bevorzugt werden, da es sich bei ihnen eher um Sicherheitsprobleme mit schwerwiegenden Auswirkungen handelt.

Gruppentitel

In der Titelspalte hat jede Gruppe eine eindeutige ID und einen nicht eindeutigen Titel. Diese basieren auf dem ASFF-Namespace für die Gruppe und der Anzahl der Erkenntnisse innerhalb dieses Namespaces im Cluster. Wenn eine Gruppierung beispielsweise den Titel: Gruppe mit: TTP (2), Effekt (1) und Ungewöhnlichem Verhalten (2), umfasst sie insgesamt fünf Erkenntnisse, bestehend aus zwei Erkenntnisse im TTP-Namespace, einer Erkenntnis im Effekt-Namespace und zwei Erkenntnissen im Namespace Ungewöhnliches Verhalten. [Eine vollständige Liste der Namespaces finden Sie unter Typen-Taxonomie für ASFF.](#)

Taktiken in einer Gruppe

In der Spalte Taktiken in einer Gruppe wird angegeben, in welche Taktikkategorie die Aktivität fällt. Die Kategorien Taktiken, Techniken und Verfahren in der folgenden Liste entsprechen der [MITRE ATT&CK-Matrix](#).

Sie können eine Taktik in der Kette auswählen, um eine Beschreibung der Taktik zu erhalten. Unter der Kette befindet sich eine Liste der innerhalb der Gruppe erkannten Taktiken. Diese Kategorien und die Aktivitäten, für die sie typischerweise stehen, lauten wie folgt:

- Erster Zugriff – Ein Angreifer versucht, in das Netzwerk einer anderen Person einzudringen.
- Ausführung – Ein Angreifer versucht, in das Netzwerk einer anderen Person einzudringen.
- Beharrlichkeit – Ein Angreifer versucht, seine Stellung zu halten.
- Eskalation von Rechten – Ein Angreifer versucht, Berechtigungen auf höherer Ebene zu erlangen.
- Umgehung der Verteidigung – Ein Angreifer versucht zu vermeiden, entdeckt zu werden.
- Zugriff auf Anmeldeinformationen – Ein Angreifer versucht, Kontonamen und Passwörter zu stehlen.
- Entdeckung – Ein Angreifer versucht, eine Umgebung zu verstehen und etwas über sie zu erfahren.
- Seitliche Bewegung – Ein Angreifer versucht, sich in einer Umgebung zu bewegen.
- Erfassung – Ein Angreifer versucht, Daten zu sammeln, die für sein Ziel von Interesse sind.
- Befehl und Steuerung – Ein Angreifer versucht, in das Netzwerk einer anderen Person einzudringen.
- Exfiltration – Ein Angreifer versucht, Daten zu stehlen.
- Auswirkung – Ein Angreifer versucht, Ihre Systeme und Daten zu manipulieren, zu unterbrechen oder zu zerstören.
- Andere – Weist auf eine Aktivität aufgrund einer Erkenntnis hin, das nicht mit den in der Matrix aufgeführten Taktiken übereinstimmt.

Entitäten innerhalb einer Gruppe

Die Spalte Entitäten enthält Details zu den spezifischen Entitäten, die innerhalb dieser Gruppierung erkannt wurden. Wählen Sie diesen Wert für eine Aufschlüsselung der Entitäten auf Grundlage der Kategorien: Identität, Netzwerk, Speicher und Datenverarbeitung. Beispiele für Entitäten in jeder Kategorie sind:

- Identität — IAM-Prinzipale und AWS-Konten, wie Benutzer und Rolle
- Netzwerk – IP-Adresse oder andere Netzwerk- und VPC-Entitäten
- Speicher – Amazon-S3-Buckets oder DDBs
- Amazon-EC2-Instances oder Kubernetes-Container berechnen

Konten innerhalb einer Gruppe

In der Spalte Konten erfahren Sie, welchen AWS Konten die Entitäten gehören, die an den Ergebnissen in der Gruppe beteiligt waren. Die AWS Konten sind nach Namen und AWS ID aufgelistet, sodass Sie Untersuchungen von Aktivitäten, die kritische Konten betreffen, priorisieren können.

Erkenntnisse innerhalb einer Gruppe

In der Spalte Erkenntnisse werden die Entitäten innerhalb einer Gruppe nach Schweregrad aufgelistet. Zu den Ergebnissen gehören GuardDuty Ergebnisse von Amazon, Amazon Inspector, AWS Sicherheitserkenntnisse und Beweise von Detective. Sie können das Diagramm auswählen, um eine genaue Anzahl der Erkenntnisse nach Schweregrad anzuzeigen.

GuardDuty Die Ergebnisse sind Teil des Detective-Kernpakets und werden standardmäßig aufgenommen. Alle anderen AWS Sicherheitsergebnisse, die von Security Hub aggregiert werden, werden als optionale Datenquelle aufgenommen. Weitere Informationen finden Sie unter [In einem Verhaltensdiagramm verwendete Quelldaten](#).

Informative Erkenntnisse in Erkenntnisgruppen

Amazon Detective identifiziert zusätzliche Informationen zu einer Erkenntnisgruppe auf der Grundlage von Daten in Ihrem Verhaltensdiagramm, die in den letzten 45 Tagen gesammelt wurden. Detective präsentiert diese Informationen als Erkenntnis mit dem Schweregrad Information. Beweise liefern unterstützende Informationen, die auf eine ungewöhnliche Aktivität oder ein unbekanntes Verhalten hinweisen, das möglicherweise verdächtig ist, wenn es innerhalb einer Erkenntnisgruppe betrachtet wird. Dazu können neu beobachtete Geolocations oder API-Aufrufe gehören, die innerhalb des Zeitraums einer Erkenntnis beobachtet wurden. Beweisergebnisse sind nur in Detective sichtbar und werden nicht an diese gesendet AWS Security Hub.

Detective bestimmt den Standort von Anfragen mithilfe von MaxMind GeoIP-Datenbanken. MaxMind meldet eine sehr hohe Genauigkeit ihrer Daten auf Landesebene, obwohl die Genauigkeit je nach Faktoren wie Land und Art des geistigen Eigentums variiert. Weitere Informationen MaxMind dazu

finden Sie unter [MaxMind IP-Geolokalisierung](#). Wenn Sie der Meinung sind, dass einige der GeolP-Daten falsch sind, können Sie unter [MaxMind Correct GeolP2](#) Data eine Korrekturanfrage an Maxmind stellen.

Sie können Beweise für verschiedene Haupttypen (z. B. IAM-Benutzer oder IAM-Rolle) beobachten. Bei einigen Arten von Nachweisen können Sie Beweise für alle Konten beobachten. Das bedeutet, dass sich Beweise auf Ihr gesamtes Verhaltensdiagramm auswirken. Wenn für alle Konten Beweiserkenntnisse festgestellt werden, wird Ihnen außerdem mindestens ein zusätzliches informatives Beweismittel desselben Typs für eine einzelne IAM-Rolle angezeigt. Wenn Sie beispielsweise die Suche Neue Geolokalisierung für alle Konten beobachtet sehen, wird Ihnen eine weitere Option für Neue Geolokalisierung für einen Prinzipal angezeigt.

Arten von Beweisen in Erkenntnisgruppen

- Neue Geolocation beobachtet
- Neue Autonomous System Organization (ASO) beobachtet
- Neuer Benutzer-Agent beobachtet
- Ein neuer API-Aufruf ausgelöst
- Für alle Konten wurde eine neue Geolocation beobachtet
- Für alle Konten wurde ein neuer IAM-Prinzipal beobachtet

Gruppenprofile finden

Wenn Sie einen Gruppentitel auswählen, wird ein Suchgruppenprofil mit zusätzlichen Details zu dieser Gruppe geöffnet. Der Detailbereich auf der Profilseite für Erkenntnisgruppen unterstützt die Anzeige von bis zu 1.000 Entitäten und Erkenntnissen für Erkenntnisgruppen (über- und untergeordnet).

Auf der Seite mit dem Gruppenprofil wird der eingestellte Zeitbereich der Gruppe angezeigt. Dies ist das Datum und die Uhrzeit vom frühesten Befund oder Nachweis in der Gruppe bis zum letzten aktualisierten Befund oder Nachweis in einer Gruppe. Sie können auch den Schweregrad der Erkenntnisgruppe sehen, der der Kategorie mit dem höchsten Schweregrad unter den Erkenntnissen in der Gruppe entspricht. Zu den weiteren Details in diesem Profilbereich gehören:

- Die Kette Involvierte Taktiken zeigt Ihnen, welche Taktiken auf die Erkenntnisse in der Gruppe zurückzuführen sind. Die Taktiken basieren auf der [MITRE ATT&CK Matrix für Unternehmen](#). Die Taktiken werden als eine Kette von farbigen Punkten dargestellt, die den typischen Verlauf

eines Angriffs von der frühesten bis zur letzten Phase darstellt. Das bedeutet, dass die Kreise ganz links in der Kette in der Regel für weniger schwerwiegende Aktivitäten stehen, bei denen ein Angreifer versucht, Zugriff auf Ihre Umgebung zu erlangen oder aufrechtzuerhalten. Umgekehrt sind Aktivitäten auf der rechten Seite am schwerwiegendsten und können Datenmanipulation oder -vernichtung beinhalten.

- Die Beziehungen, die diese Gruppe zu anderen Gruppen unterhält. Gelegentlich können eine oder mehrere Erkenntnisgruppen, die zuvor keinen Zusammenhang hatten, auf der Grundlage eines neu entdeckten Zusammenhangs zu einer neuen Gruppe zusammengeführt werden, z. B., wenn es sich um eine Erkenntnis handelt, an der Entitäten aus den vorhandenen Gruppen beteiligt sind. In diesem Fall deaktiviert Amazon Detective die übergeordneten Gruppen und erstellt eine untergeordnete Gruppe. Sie können die Herkunft jeder Gruppe bis zu ihren übergeordneten Gruppen zurückverfolgen. Gruppen können die folgenden Beziehungen haben:
 - Erkenntnisgruppe untergeordnet – Eine Erkenntnisgruppe, die erstellt wird, wenn ein Befund, der in zwei anderen Erkenntnisgruppen enthalten ist, in eine neue Erkenntnis involviert ist. Die übergeordneten Erkenntnisgruppen werden für jede untergeordnete Gruppe aufgeführt.
 - Erkenntnisgruppe übergeordnet – Eine Erkenntnisgruppe ist eine übergeordnete Gruppe, wenn aus ihr eine untergeordnete Gruppe erstellt wurde. Handelt es sich bei der Erkenntnisgruppe um eine übergeordnete Gruppe, werden die zugehörigen untergeordneten Gruppen zusammen mit ihr aufgeführt. Der Status einer übergeordneten Gruppe wird inaktiv, wenn sie zu einer aktiven untergeordneten Gruppe zusammengeführt wird.

Es gibt zwei Informationsregisterkarten, über die Profilbereich geöffnet werden. Auf den Registerkarten Beteiligte Entitäten und Beteiligte Erkenntnisse können Sie weitere Details zur Gruppe einsehen.

Verwenden Sie Untersuchung durchführen, um einen Untersuchungsbericht zu erstellen. Der generierte Bericht beschreibt ein anomales Verhalten, das auf eine Beeinträchtigung hindeutet.

Profilbereich innerhalb von Gruppen

Beteiligte Entitäten

Konzentriert sich auf die Entitäten in der Erkenntnisgruppe, einschließlich der Erkenntnisse innerhalb der Gruppe, mit denen die einzelnen Entitäten verknüpft sind. Die jeder Entität angehängten Tags werden ebenfalls angezeigt, sodass Sie wichtige Entitäten anhand der Kennzeichnung schnell identifizieren können. Wählen Sie eine Entität aus, um ihr Entitätsprofil anzuzeigen.

Involvierte Erkenntnisse

Enthält Einzelheiten zu jeder Erkenntnis, einschließlich des Schweregrads der Erkenntnis, jeder beteiligten Entität und wann die Erkenntnis zum ersten und letzten Mal festgestellt wurde. Wählen Sie einen Befundtyp in der Liste aus, um einen Bereich mit den Erkenntnisdetails mit zusätzlichen Informationen zu diesem Erkenntnis zu öffnen. Im Bereich Involvierte Erkenntnisse werden Ihnen möglicherweise Informative Erkenntnisse angezeigt, die auf Erkenntnissen von Detective aus Ihrem Verhaltensdiagramm basieren.

Visualisierung von Erkenntnisgruppen

Amazon Detective bietet eine interaktive Visualisierung von Erkenntnisgruppen. Diese Visualisierung soll Ihnen helfen, Probleme schneller und gründlicher mit weniger Aufwand zu untersuchen. Im Bereich Visualisierung von Erkenntnisgruppen werden die Erkenntnisse und Entitäten angezeigt, die an einer Erkenntnisgruppe beteiligt sind. Sie können diese interaktive Visualisierung verwenden, um die Auswirkungen der Erkenntnisgruppe zu analysieren, zu verstehen und zu bewerten. In diesem Bereich können Sie die Informationen in den Tabellen Involvierte Entitäten und Involvierte Erkenntnisse visualisieren. In der visuellen Präsentation können Sie Erkenntnisse oder Entitäten für die weitere Analyse auswählen.

Erkenntnisgruppen in Detective mit aggregierten Erkenntnissen sind eine Gruppe von Erkenntnissen, die mit derselben Art von Ressource verknüpft sind. Mit aggregierten Erkenntnissen können Sie schnell die Zusammensetzung einer Erkenntnisgruppe einschätzen und Sicherheitsprobleme schneller interpretieren. Im Bereich mit den Details zu den Erkenntnisgruppen werden ähnliche Erkenntnisse kombiniert, und Sie können die Erkenntnisse erweitern, um relativ ähnliche Erkenntnisse w zusammen anzuzeigen. Beispiel: Ein Evidenzknoten, in dem informative Erkenntnisse und mittlere Erkenntnisse desselben Typs zusammengefasst sind. Derzeit können Sie Titel, Quelle, Art und Schweregrad von Erkenntnisgruppen mit aggregierten Erkenntnissen anzeigen.

In diesem interaktiven Bereich können Sie:

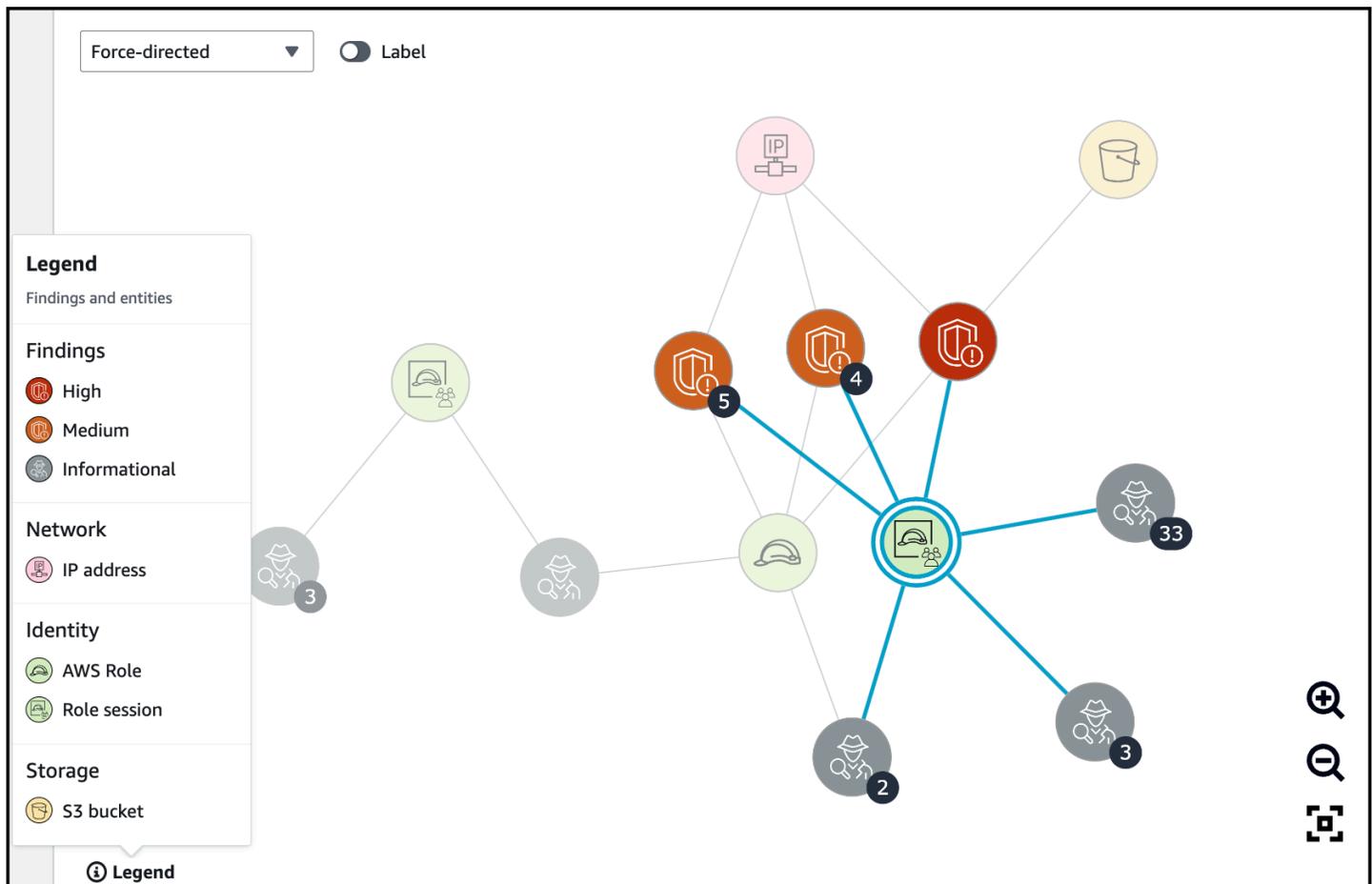
- Verwenden Sie Untersuchung durchführen, um einen Untersuchungsbericht zu erstellen. Der generierte Bericht beschreibt das ungewöhnliche Verhalten, das auf eine Gefährdung hindeutet.
- Hier finden Sie weitere Informationen zur Suche nach Gruppen mit aggregierten Erkenntnissen, um die beteiligten Beweise, Entitäten und Erkenntnisse zu analysieren.
- Sehen Sie sich die Bezeichnungen der Entitäten und Erkenntnisse an, um die betroffenen Entitäten mit potenziellen Sicherheitsproblemen zu identifizieren. Sie können das Label deaktivieren.

- Ordnen Sie die Entitäten und Erkenntnisse neu an, um ihre Zusammenhänge besser zu verstehen. Isolieren Sie Entitäten und Erkenntnisse aus einer Gruppe, indem Sie das ausgewählte Element in der Erkenntnisgruppe verschieben.
- Wählen Sie die Beweise, Entitäten und Erkenntnisse aus, um weitere Details zu ihnen anzuzeigen. Wählen Sie zur Auswahl mehrerer Elemente **command/control** und die Elemente aus oder verschieben Sie sie per Drag-and-Drop mit dem Mauszeiger.
- Passen Sie das Layout so an, dass alle Entitäten und Erkenntnisse in das Erkenntnisgruppenfenster passen. Sehen Sie sich an, welche Entitätstypen in einer Erkenntnisgruppe vorherrschen.

Note

Der Bereich Visualisierung für Erkenntnisgruppen unterstützt die Anzeige von Erkenntnisgruppen mit bis zu 100 Entitäten und Erkenntnissen.

Sie können „Layout auswählen“ wählen, um die Erkenntnisse und Entitäten in einem Kreis-, Kraftgesteuerten oder Rasterlayout anzuzeigen. Beim Layout Kraftgesteuert werden die Entitäten und Erkenntnisse so positioniert, dass die Links eine gleichbleibende Länge zwischen den Elementen haben und gleichmäßig verteilt sind. Dies trägt dazu bei, Überlappungen zu reduzieren. Das von Ihnen gewählte Layout definiert die Platzierung der Erkenntnisse im Bereich Visualisierung.



Die dynamische Legende ändert sich je nach Entitäten und Erkenntnissen in Ihrem aktuellen Diagramm. Sie hilft Ihnen zu identifizieren, wofür jedes visuelle Element steht.

Erkenntnisgruppenübersicht basierend auf generativer KI

Standardmäßig stellt Amazon Detective automatisch Übersichten einzelner Erkenntnisgruppen bereit. Die Übersichten basieren auf Modellen der generativen künstlichen Intelligenz (generative KI), die auf [Amazon Bedrock](#) gehostet werden.

Mithilfe von Erkenntnisgruppen können Sie mehrere Sicherheitserkenntnisse untersuchen, da sie sich auf ein potenzielles Sicherheitsereignis beziehen und potenzielle Bedrohungsakteure identifizieren. Die Suche nach Gruppenübersichten zum Auffinden von Gruppen baut auf diesen Funktionen auf. Erkenntnisgruppenübersichten verwenden die Daten für eine Erkenntnisgruppe, analysieren die Beziehungen zwischen den Erkenntnissen und den betroffenen Ressourcen schnell und fassen anschließend potenzielle Bedrohungen in natürlicher Sprache zusammen. Sie können diese Übersichten nutzen, um größere Sicherheitsbedrohungen zu identifizieren, die Effizienz der Ermittlungen zu verbessern und die Reaktionszeiten zu verkürzen.

Note

Erkenntnisgruppenübersichten, die auf generativer KI basieren, liefern möglicherweise, aber nicht immer, vollständig genaue Informationen. Weitere Informationen finden Sie in der [AWS - Richtlinie für verantwortungsvolle KI](#).

Erkenntnisgruppenübersichten überprüfen

In der Erkenntnisübersichten für eine Erkenntnisgruppe finden Sie eine klare und detaillierte Erläuterung eines Sicherheitsereignisses. In natürlicher Sprache enthält die Erklärung einen prägnanten Titel, eine Übersicht der beteiligten Ressourcen und kuratierte Informationen zu diesen Ressourcen.

So überprüfen Sie eine Erkenntnisgruppenübersicht

1. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich Gruppen finden aus.
3. Wählen Sie in der Tabelle Erkenntnisgruppen die Erkenntnisgruppe aus, für die Sie eine Übersicht anzeigen möchten. Eine Detailseite wird angezeigt.

Auf der Detailseite können Sie den ÜbersichtsBereich verwenden, um eine generierte, beschreibende Übersicht der wichtigsten Erkenntnisse in der Erkenntnisgruppe zu überprüfen. Sie können auch eine Analyse der wichtigsten Bedrohungsereignisse in der Erkenntnisgruppe überprüfen, die Sie dann weiter untersuchen können. Um die generierte Übersicht zu Ihren Notizen oder einem Ticketsystem hinzuzufügen, wählen Sie das Kopiersymbol im Bereich. Dadurch wird die Übersicht in Ihre Zwischenablage kopiert. Sie können auch Ihr Feedback zur Ausgabe der Erkenntnisgruppenübersicht in der Übersicht angeben, was in Zukunft für ein besseres Nutzererlebnis sorgen kann. Um Ihr Feedback zu teilen, wählen Sie je nach Art Ihres Feedbacks das Symbol „Daumen hoch“ oder „Daumen runter“.

Note

Wenn Sie Feedback zur Übersicht der Erkenntnisgruppe geben, wird Ihr Feedback nicht für die Modelloptimierung verwendet. Wir verwenden es nur, um sicherzustellen, dass die Eingabeaufforderungen in Detective effektiv gestaltet werden.

**Summary - new Info****Credentials exfiltration from i-0e5f7e596391b28eb using role privilegedRole**

Instance i-0e5f7e596391b28eb had newly observed API calls and user agents for role privilegedRole.

Credentials for role privilegedRole on i-0e5f7e596391b28eb were exfiltrated and used from account [REDACTED] and IP [REDACTED].

The exfiltrated credentials were used to access S3 bucket private-bucket-[REDACTED].

i-0e5f7e596391b28eb was vulnerable to CVE-2021-44228 and CVE-2021-45046.



Die Übersicht der Erkenntnisgruppe wird deaktiviert

Standardmäßig ist die Suche nach Gruppenübersicht für die Suche nach Gruppen aktiviert. Sie können die Erkenntnisgruppenübersicht jederzeit deaktivieren. Wenn Sie deaktivieren, können Sie später wieder aktivieren.

So deaktivieren Sie die Erkenntnisgruppenübersicht

1. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Klicken Sie im Navigationsbereich auf Präferenzen.
3. Wählen Sie unter Erkenntnisgruppenübersicht die Option Bearbeiten aus.
4. Schalten Sie Aktiviert aus.

5. Wählen Sie Speichern.

Die Erkenntnisgruppenübersicht wird aktiviert

Wenn Sie die Erkenntnisgruppenübersicht für Erkenntnisgruppen zuvor deaktiviert haben, können Sie sie jederzeit wieder aktivieren.

So aktivieren Sie die Erkenntnisgruppenübersicht

1. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Klicken Sie im Navigationsbereich auf Präferenzen.
3. Wählen Sie unter Erkenntnisgruppenübersicht die Option Bearbeiten aus.
4. Aktivieren Sie Aktiviert.
5. Wählen Sie Speichern.

Unterstützte Regionen

Finding Group Summary ist in den folgenden AWS Regionen verfügbar.

- USA Ost (Nord-Virginia)
- USA West (Oregon)
- Asien-Pazifik (Tokio)
- Europa (Frankfurt)

Analysieren von Entitäten in Amazon Detective

Eine Entität ist ein einzelnes Objekt, das aus den Quelldaten extrahiert wurde. Beispiele hierfür sind eine bestimmte IP-Adresse, eine Amazon EC2 EC2-Instance oder AWS ein Konto. Eine Liste der Entitätstypen finden Sie unter [the section called “Arten von Entitäten in der Datenstruktur des Verhaltensdiagramms”](#).

Ein Amazon-Detective-Entitätsprofil ist eine einzelne Seite, die detaillierte Informationen über die Entität und ihre Aktivitäten enthält. Sie können ein Entitätsprofil verwenden, um unterstützende Informationen für eine Untersuchung einer Erkenntnis oder im Rahmen einer allgemeinen Suche nach verdächtigen Aktivitäten zu erhalten.

Inhalt

- [Identifizieren einer interessanten Entität mithilfe der Übersichtsseite](#)
- [Verwenden von Entitätsprofilen](#)
- [Profilbereich anzeigen und mit ihnen interagieren](#)
- [Direkt zu einem Entitätsprofil navigieren oder eine Übersicht finden](#)
- [Verwaltung des Zeitbereichs](#)
- [Details zu den zugehörigen Erkenntnissen ansehen](#)
- [Details für Entitäten mit hohem Volumen anzeigen](#)

Identifizieren einer interessanten Entität mithilfe der Übersichtsseite

Verwenden Sie die Übersichtsseite in Amazon Detective, um Entitäten zu identifizieren und den Ursprung der Aktivitäten in den letzten 24 Stunden zu untersuchen. Die Amazon-Detective-Übersichtsseite hilft Ihnen, Entitäten zu identifizieren, die mit bestimmten Arten ungewöhnlicher Aktivitäten in Verbindung stehen. Dies ist einer von mehreren möglichen Ausgangspunkten für eine Untersuchung.

Um die Übersichtsseite anzuzeigen, wählen Sie im Navigationsbereich von Detective die Option Übersicht aus. Die Übersichtsseite wird standardmäßig auch angezeigt, wenn Sie die Detective-Konsole zum ersten Mal öffnen.

Auf der Übersichtsseite können Sie Entitäten identifizieren, die die folgenden Kriterien erfüllen:

- Untersuchungen, die auf potenzielle Sicherheitsereignisse hinweisen, die von Detective identifiziert wurden
- Entitäten, die an Aktivitäten in neu beobachteten Geolokationen beteiligt sind
- Entitäten, die die meisten API-Aufrufe getätigt haben
- EC2-Instances mit dem größten Datenverkehrsvolumen
- Container-Cluster mit der größten Anzahl von Containern

Von jedem Bereich der Übersichtsseite aus können Sie zum Profil einer ausgewählten Entität wechseln.

Wenn Sie sich die Übersichtsseite ansehen, können Sie den Zeitbereich für den Umfang anpassen, sodass Sie sich die Aktivität für einen beliebigen 24-Stunden-Zeitraum der letzten 365 Tage ansehen können. Wenn Sie das Startdatum und die Startzeit ändern, werden das Enddatum und die Endzeit automatisch auf 24 Stunden nach der ausgewählten Startzeit aktualisiert.

Mit Detective können Sie auf historische Ereignisdaten von bis zu einem Jahr zugreifen. Diese Daten sind über eine Reihe von Visualisierungen verfügbar, die Veränderungen in Art und Umfang der Aktivitäten in einem ausgewählten Zeitfenster zeigen. Detective verknüpft diese Änderungen mit GuardDuty Ergebnissen.

Weitere Informationen zu Quelldaten in Detective finden Sie unter [In einem Verhaltensdiagramm verwendete Quelldaten](#).

Untersuchungen

Untersuchungen zeigen Ihnen die potenziellen Sicherheitsereignisse, die Detective identifiziert hat. Im Bereich „Untersuchungen“ können Sie sich kritische Untersuchungen und die entsprechenden AWS -Rollen und Benutzer ansehen, die über einen bestimmten Zeitraum von Sicherheitsereignissen betroffen waren. Bei der Untersuchung werden Indikatoren für eine Gefährdung zusammengefasst, um festzustellen, ob eine AWS Ressource an ungewöhnlichen Aktivitäten beteiligt ist, die auf böses Verhalten und dessen Auswirkungen hinweisen könnten.

Wählen Sie Alle Untersuchungen anzeigen aus, um Erkenntnisse, Gruppen und Ressourcendetails zu überprüfen und so Ihre Sicherheitsuntersuchung zu beschleunigen. Untersuchungen werden je nach ausgewähltem Zeitbereich angezeigt. Sie können den Umfang so anpassen, dass die Untersuchungen in den letzten 365 Tagen innerhalb von 24 Stunden angezeigt werden. Sie können direkt zu Kritische Untersuchungen wechseln, um einen detaillierten Untersuchungsbericht zu sehen.

Wenn Sie eine AWS Rolle oder einen Benutzer identifizieren, der verdächtige Aktivitäten zu haben scheint, können Sie direkt vom Bereich Ermittlungen zu der Rolle oder dem Benutzer wechseln, um Ihre Untersuchung fortzusetzen. Wechseln Sie zu einer Rolle oder einem Benutzer und klicken Sie auf Untersuchung ausführen, um einen Untersuchungsbericht zu erstellen. Sobald Sie eine Untersuchung für eine Rolle oder einen Benutzer durchgeführt haben, wird die Rolle oder der Benutzer auf die Registerkarte Untersucht verschoben.

Neu beobachtete Geolocations

Neu beobachtete Geolocations heben geografische Standorte hervor, von denen die Aktivitäten in den letzten 24 Stunden ausgegangen sind, die aber im Bezugszeitraum davor nicht beobachtet wurden.

Der Bereich umfasst bis zu 100 Geolocations. Die Standorte sind auf der Karte markiert und in der Tabelle unter der Karte aufgeführt.

Für jeden Standort zeigt die Tabelle die Anzahl der fehlgeschlagenen und erfolgreichen API-Aufrufe an, die in den letzten 24 Stunden von diesem Standort aus getätigt wurden.

Sie können jede Geolokalisierung erweitern, um die Liste der Benutzer und Rollen anzuzeigen, die API-Aufrufe von dieser Geolocation aus getätigt haben. In der Tabelle sind für jeden Prinzipal der Typ und die zugehörigen AWS-Konto aufgeführt.

Wenn Sie einen Benutzer oder eine Rolle identifizieren, die Ihnen verdächtig erscheinen, können Sie direkt vom Bereich zum Benutzer- oder Rollenprofil wechseln, um Ihre Untersuchung fortzusetzen. Um zu einem Profil zu wechseln, wählen Sie die Benutzer- oder Rollen-ID aus.

Detective bestimmt den Standort von Anfragen mithilfe von MaxMind GeoIP-Datenbanken. MaxMind meldet eine sehr hohe Genauigkeit ihrer Daten auf Landesebene, obwohl die Genauigkeit je nach Faktoren wie Land und Art des geistigen Eigentums variiert. Weitere Informationen MaxMind dazu finden Sie unter [MaxMind IP-Geolokalisierung](#). Wenn Sie der Meinung sind, dass einige der GeoIP-Daten falsch sind, können Sie unter [MaxMind Correct GeoIP2 Data](#) eine Korrekturanfrage an Maxmind stellen.

Aktive Erkenntnisgruppen in den letzten 7 Tagen

Aktive Erkenntnisgruppen der letzten 7 Tage zeigt Ihnen korrelierte Gruppierungen von Detective-Erkenntnissen, Entitäten und Beweisen in Ihrer Umgebung, die über einen bestimmten Zeitraum aufgetreten sind. Diese Gruppierungen korrelieren ungewöhnliche Aktivitäten, die auf böswilliges

Verhalten hinweisen könnten. Auf der Übersichtsseite werden bis zu fünf Gruppen angezeigt, sortiert nach den Gruppen mit den wichtigsten Erkenntnissen, die in der letzten Woche aktiv waren.

Sie können Werte in den Inhalten Taktik, Konto, Ressource und Erkenntnisse auswählen, um weitere Details zu sehen.

Erkenntnisgruppen werden täglich generiert. Wenn Sie eine interessante Erkenntnisgruppe identifizieren, können Sie den Titel auswählen, um zu einer detaillierten Ansicht eines Gruppenprofils zu gelangen und Ihre Untersuchung fortzusetzen.

Rollen und Benutzer mit dem höchsten API-Aufrufvolumen

Rollen und Benutzer mit dem höchsten API-Aufrufvolumen identifiziert die Benutzer und Rollen, die in den letzten 24 Stunden die meisten API-Aufrufe getätigt haben.

Der Bereich kann bis zu 100 Benutzer und Rollen enthalten. Für jeden Benutzer oder jede Rolle können Sie den Typ (Benutzer oder Rolle) und das zugehörige Konto sehen. Sie können auch die Anzahl der API-Aufrufe sehen, die von diesem Benutzer oder dieser Rolle in den letzten 24 Stunden getätigt wurden.

Standardmäßig werden dienstbezogene Rollen angezeigt. Rollen, die mit Diensten verknüpft sind, können zu großen AWS CloudTrail Aktivitäten führen, wodurch die Hauptpersonen, die Sie weiter untersuchen möchten, verdrängt werden. Sie können die Option Serviceverknüpfte Rollen anzeigen deaktivieren, um servicebezogene Rollen aus der Ansicht der Übersichtsseite herauszufiltern.

Sie können eine Datei mit kommagetrennten Werten (.csv) exportieren, die die Daten in diesem Bereich enthält.

Es gibt auch einen Zeitplan für das API-Aufrufvolumen der letzten 7 Tage. Anhand des Zeitplans können Sie feststellen, ob das Volumen der API-Aufrufe für diesen Prinzipal ungewöhnlich ist.

Wenn Sie einen Benutzer oder eine Rolle identifizieren, für die das API-Aufrufvolumen verdächtig erscheint, können Sie direkt vom Bereich zum Benutzer- oder Rollenprofil wechseln, um Ihre Untersuchung fortzusetzen. Sie können auch das Profil des Kontos einsehen, das dem Benutzer oder der Rolle zugeordnet ist. Um ein Profil anzuzeigen, wählen Sie den Benutzer, die Rolle oder die Konto-ID aus.

EC2-Instances mit dem höchsten Verkehrsvolumen

EC2-Instances mit dem höchsten Verkehrsvolumen identifizieren die EC2-Instances, die in den letzten 24 Stunden das größte Gesamtverkehrsvolumen hatten.

Der Bereich kann bis zu 100 EC2-Instances enthalten. Für jede EC2-Instance können Sie das zugehörige Konto und die Anzahl der eingehenden Bytes, ausgehenden Bytes und die Gesamtzahl der Bytes der letzten 24 Stunden sehen.

Sie können eine CSV-Datei (komma-getrennte Werte) exportieren, die die Daten in diesem Bereich enthält.

Sie können auch eine Zeitleiste sehen, in der der eingehende und ausgehende Verkehr der letzten 7 Tage angezeigt wird. Anhand der Zeitleiste können Sie feststellen, ob das Verkehrsaufkommen für diese EC2-Instance ungewöhnlich ist.

Wenn Sie eine EC2-Instance mit verdächtigem Datenverkehrsvolumen identifizieren, können Sie direkt vom Bereich zum EC2-Instance-Profil wechseln, um Ihre Untersuchung fortzusetzen. Sie können auch das Profil des Kontos einsehen, dem die EC2-Instance gehört. Um ein Profil anzuzeigen, wählen Sie die EC2-Instance oder Konto-ID aus.

Container-Cluster mit den meisten Kubernetes-Pods

Containercluster mit den meisten erstellten Kubernetes-Pods identifizieren die Cluster, in denen in den letzten 24 Stunden die meisten Container ausgeführt wurden.

Dieser Bereich umfasst bis zu 100 Cluster, die danach geordnet sind, mit welchen Clustern die meisten Erkenntnisse verknüpft wurden. Für jeden Cluster können Sie das zugehörige Konto, die aktuelle Anzahl von Containern in diesem Cluster und die Anzahl der mit diesem Cluster verknüpften Erkenntnisse in den letzten 24 Stunden sehen. Sie können eine CSV-Datei (komma-getrennte Werte) exportieren, die die Daten in diesem Bereich enthält.

Wenn Sie einen Cluster mit aktuellen Erkenntnissen identifizieren, können Sie direkt vom Bereich zum Clusterprofil wechseln, um Ihre Untersuchung fortzusetzen. Sie können auch zum Profil des Accounts wechseln, dem der Cluster gehört. Um zu einem Profil zu wechseln, wählen Sie den Clusternamen oder die Konto-ID aus.

Benachrichtigung über den ungefähren Wert

Wenn bei Rollen und Benutzern mit dem meisten API-Aufrufvolumen und bei EC2-Instances mit dem meisten Datenverkehrsvolumen auf einen Wert ein Sternchen (*) folgt, bedeutet dies, dass es sich bei dem Wert um einen Näherungswert handelt. Der wahre Wert ist entweder gleich oder größer als der angezeigte Wert.

Dies liegt an der Methode, mit der Detective das Volumen für jedes Zeitintervall berechnet. Auf der Übersichtsseite ist das Zeitintervall eine Stunde.

Für jede Stunde berechnet Detective das Gesamtvolumen für die 1.000 Benutzer, Rollen oder EC2-Instances mit dem größten Volumen. Es schließt die Daten für die verbleibenden Benutzer, Rollen oder EC2-Instances aus.

Wenn eine Ressource manchmal unter den Top 1.000 war und manchmal nicht, beinhaltet das berechnete Volumen für diese Ressource möglicherweise nicht alle Daten. Die Daten für die Zeitintervalle, in denen sie nicht zu den obersten 1.000 gehörte, werden nicht berücksichtigt.

Beachten Sie, dass dies nur für die Übersichtsseite gilt. Das Profil für den Benutzer, die Rolle oder die EC2-Instance enthält genaue Details.

Verwenden von Entitätsprofilen

Ein Entitätsprofil wird angezeigt, wenn Sie eine der folgenden Aktionen ausführen:

- Wählen Sie in der GuardDuty Amazon-Konsole die Option, um eine Entität zu untersuchen, die mit einem ausgewählten Ergebnis zusammenhängt.

Siehe [the section called “Von einer anderen Konsole aus wechseln”](#).

- Gehen Sie zur Detective-URL für das Entitätsprofil.

Siehe [the section called “Navigation mithilfe einer URL”](#).

- Verwenden Sie die Detective-Suche in der Detective-Konsole, um nach einer Entität zu suchen.
- Wählen Sie einen Link zum Entitätsprofil aus einem anderen Entitätsprofil oder aus einer Erkenntnisübersicht.

Geltungsbereich eines Entitätsprofils

Wenn Sie direkt zu einem Entitätsprofil navigieren, ohne den Zeitbereich anzugeben, wird die Geltungsdauer auf die letzten 24 Stunden festgelegt.

Wenn Sie von einem anderen Entitätsprofil zu einem Entitätsprofil navigieren, bleibt die aktuell ausgewählte Gültigkeitsdauer erhalten.

Wenn Sie von einer Erkenntnisübersicht aus zu einem Entitätsprofil navigieren, wird die Gültigkeitsdauer auf das Suchzeitfenster festgelegt.

Informationen zur Anpassung der Gültigkeitsdauer zur Begrenzung der in Entitätsprofilen angezeigten Daten finden Sie unter [Verwaltung der Gültigkeitsdauer](#).

Kennung und Typ der Entität

Oben im Profil befinden sich die Entitäts-ID und der Entitätstyp. Jeder Entitätstyp hat ein entsprechendes Symbol, das einen visuellen Hinweis auf den Profiltyp bietet.

Involvierte Erkenntnisse

Jedes Profil enthält eine Liste der Erkenntnisse, an denen das Unternehmen während des Berichtszeitraums beteiligt war.

Sie können die Details für jede Erkenntnis einsehen, den Zeitrahmen für den Umfang ändern, sodass er dem Zeitfenster für die Erkenntnisse entspricht, und in der Erkenntnisübersicht nach anderen beteiligten Ressourcen suchen.

Siehe [the section called “Erkenntnisse für eine Entität anzeigen”](#).

Erkenntnisgruppen, an denen diese Entität beteiligt ist

Jedes Profil enthält eine Liste von Erkenntnisgruppen, in denen eine Entität enthalten ist.

Eine Erkenntnisgruppe besteht aus Erkenntnissen, Entitäten und Beweisen, die Detective zu einer Gruppe zusammenfasst, um mehr Kontext zu möglichen Sicherheitsproblemen bereitzustellen.

Weitere Informationen zu Gruppen finden Sie unter [the section called “Gruppen finden”](#).

Profilbereich mit Entitätsdetails und Analyseergebnissen

Jedes Entitätsprofil enthält mindestens eine Gruppe von einer oder mehreren Registerkarten. Jede Registerkarte enthält mindestens ein Profilbereich. Jeder Profilbereich enthält Text und Visualisierungen, die aus den Verhaltensdiagrammdateien generiert werden. Die spezifischen Registerkarten und Profilbereich sind auf den Entitätstyp zugeschnitten.

Bei den meisten Entitäten bietet der Bereich oben auf der ersten Registerkarte allgemeine zusammenfassende Informationen über die Entität.

In anderen Profilbereichen werden verschiedene Arten von Aktivitäten hervorgehoben. Für ein Unternehmen, das an einer Erkenntnis beteiligt ist, können die Informationen in den Profilbereichen der Entität zusätzliche Belege für den Abschluss einer Untersuchung liefern. Jeder Profilbereich bietet

Zugang zu Anleitungen zur Verwendung der Informationen. Weitere Informationen finden Sie unter [the section called “Verwendung von Anleitungen durch den Profilbereich”](#).

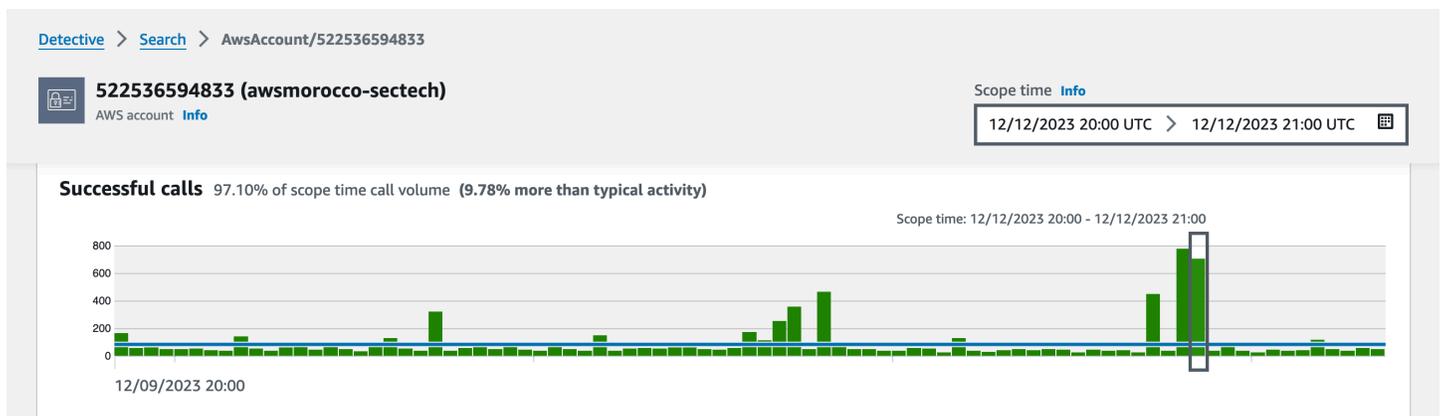
Weitere Informationen zu den Profilbereichen, den darin enthaltenen Datentypen und den verfügbaren Optionen für die Interaktion mit ihnen finden Sie unter [the section called “Profilbereich anzeigen und mit ihnen interagieren”](#).

In einem Entitätsprofil navigieren

Ein Entitätsprofil umfasst einen Satz von einer oder mehreren Registerkarten. Jede Registerkarte enthält mindestens ein Profilbereich. Jeder Profilbereich enthält Text und Visualisierungen, die aus den Verhaltensdiagrammdateien generiert werden.

Wenn Sie durch eine Profilregisterkarte nach unten scrollen, bleiben die folgenden Informationen oben im Profil sichtbar:

- Entitätstyp
- Entitäts-ID
- Bereichsname



Profilbereich anzeigen und mit ihnen interagieren

Jedes Entitätsprofil auf der Amazon-Detective-Konsole besteht aus einer Reihe von Profilbereichen. Ein Profilbereich ist eine Visualisierung, die allgemeine Details enthält oder bestimmte Aktivitäten hervorhebt, die mit einer Entität verbunden sind. In Profilbereichen werden verschiedene Arten von Visualisierungen verwendet, um verschiedene Arten von Informationen darzustellen. Sie können auch Links zu zusätzlichen Details oder zu anderen Profilen enthalten.

Jeder Profilbereich soll Analysten dabei helfen, Antworten auf spezifische Fragen zu Unternehmen und den damit verbundenen Aktivitäten zu finden. Anhand der Antworten auf diese Fragen lässt sich schlussfolgern, ob die Aktivität eine echte Bedrohung darstellt.

Inhalt

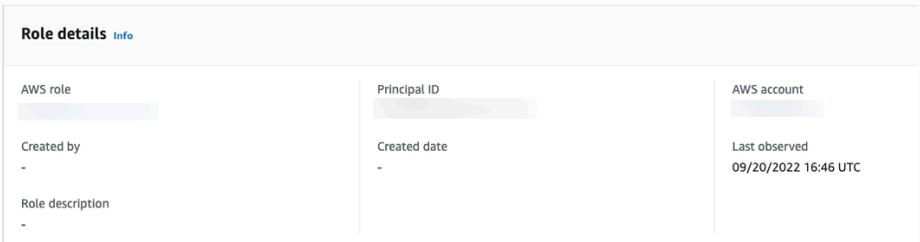
- [Inhalt des Profilbereichs](#)
- [Festlegen der Einstellungen für einen Profilbereich](#)
- [Von einem Profilbereich zu einer anderen Konsole wechseln](#)
- [Von einem Profilbereich zu einem anderen Entitätsprofil wechseln](#)
- [Erkunden von Aktivitätsdetails in einem Profilbereich](#)

Inhalt des Profilbereichs

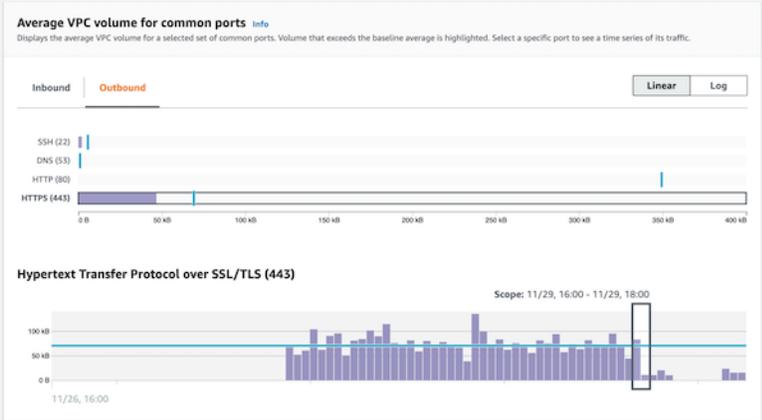
In Profilbereichen werden verschiedene Arten von Visualisierungen verwendet, um verschiedene Arten von Informationen darzustellen.

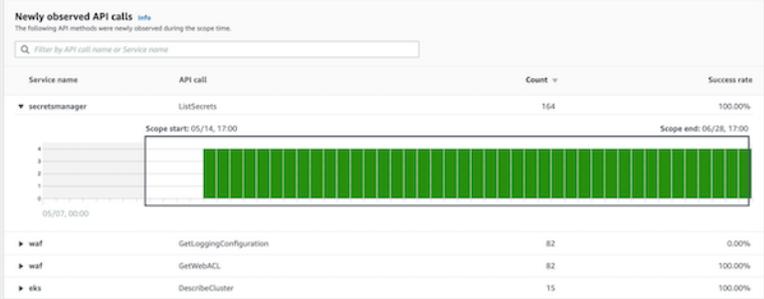
Arten von Informationen in einem Profilbereich

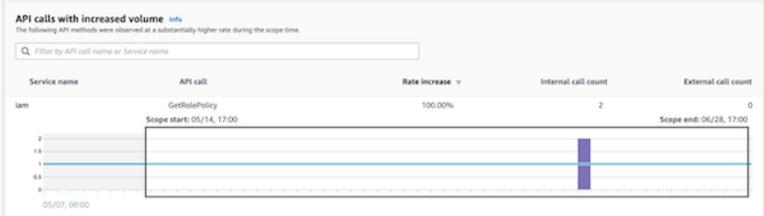
Profilbereiche enthalten in der Regel die folgenden Datentypen.

Datentyp des Bereichs	Beschreibung
Allgemeine Informationen zu einer Erkenntnis oder Entität	<p>Der einfachste Bereichstyp bietet einige grundlegende Informationen zu einer Entität.</p> <p>Zu den in einem Informationsbereich enthaltenen Informationen gehören beispielsweise die Kennung, der Name, der Typ und das Erstellungsdatum.</p>  <p>Die meisten Entitätsprofile enthalten einen Informationsbereich für diese Entität.</p>

Datentyp des Bereichs	Beschreibung
Allgemeine Übersicht der Aktivitäten im Laufe der Zeit	<p>Zeigt eine Übersicht der Aktivitäten einer Entität im Zeitverlauf an.</p> <p>Diese Art von Bereich bietet einen Gesamtüberblick darüber, wie sich eine Entität während des Zeitbereichs verhält.</p>  <p>Hier finden Sie einige Beispiele für zusammenfassende Daten, die in den Profilbereichen von Detective bereitgestellt werden:</p> <ul style="list-style-type: none"> • Fehlgeschlagene und erfolgreiche API-Aufrufe • Eingehendes und ausgehendes VPC-Volumen

Datentyp des Bereichs	Beschreibung
Übersicht der Aktivitäten, gruppiert nach Werten	<p>Zeigt eine Übersicht der Aktivitäten für eine Entität an, gruppiert nach bestimmten Werten.</p> <p>Sie können diese Art von Profilbereich im Profil für eine EC2-Instance sehen. Im Profilbereich wird das durchschnittliche Volumen der VPC-Datendurchfluss-Protokolldaten zu und von einer EC2-Instance für allgemeine Ports angezeigt, die bestimmten Arten von Diensten zugeordnet sind.</p>  <p>The screenshot displays two charts. The top chart, titled 'Average VPC volume for common ports', shows a bar chart for 'Outbound' traffic. The x-axis represents volume in kB, ranging from 0 to 400. The y-axis lists ports: SSH (22), DNS (53), HTTP (80), and HTTPS (443). The HTTPS bar is significantly longer than the others, indicating the highest volume. The bottom chart, titled 'Hypertext Transfer Protocol over SSL/TLS (443)', is a time-series bar chart showing traffic volume over time. The x-axis is labeled 'Scope: 11/29, 16:00 - 11/29, 18:00'. The y-axis shows volume in kB, with a horizontal blue line representing the baseline. A red box highlights a specific data point in the chart.</p>

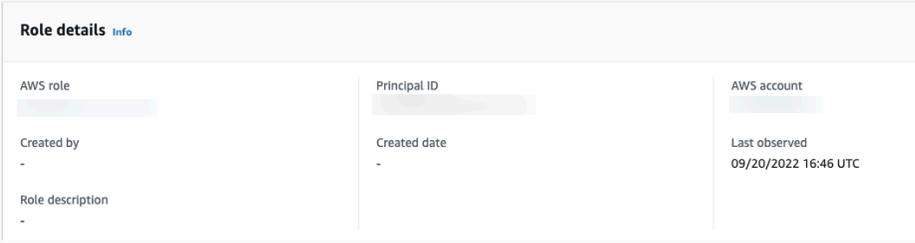
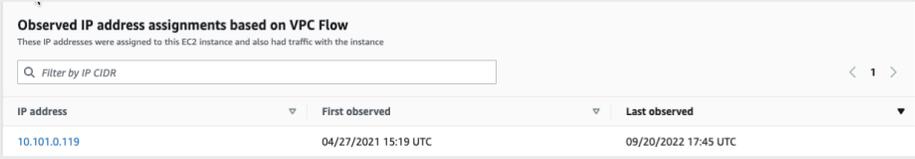
Datentyp des Bereichs	Beschreibung
<p>Aktivität, die erst während des Zeitbereichs gestartet wurde</p>	<p>Während einer Untersuchung ist es wichtig zu sehen, welche Aktivität erst in einem bestimmten Zeitraum stattgefunden hat.</p> <p>Gibt es zum Beispiel API-Aufrufe, geografische Standorte oder Benutzeragenten, die zuvor noch nicht gesehen wurden?</p>  <p>Befindet sich das Verhaltensdiagramm noch im Trainingsmodus, zeigt der Profilbereich eine Benachrichtigung an. Die Meldung wird entfernt, wenn das Verhaltensdiagramm Daten für mindestens zwei Wochen gesammelt hat. Weitere Informationen zum Trainingsmodus finden Sie unter the section called "Trainingszeit für neue Verhaltensdiagramme".</p>

Datentyp des Bereichs	Beschreibung
<p>Aktivität, die sich während des Gültigkeitszeitraums erheblich geändert hat</p>	<p>Ähnlich wie in den neuen Aktivitätsbereiche können auch in Profilbereichen Aktivitäten angezeigt werden, die sich während des Gültigkeitszeitraums erheblich geändert haben.</p> <p>Beispielsweise kann ein Benutzer regelmäßig ein paar Mal pro Woche einen bestimmten API-Aufruf tätigen. Wenn derselbe Benutzer plötzlich mehrmals an einem Tag denselben Aufruf tätigt, kann dies ein Hinweis auf böswillige Aktivitäten sein.</p>  <p>Befindet sich das Verhaltensdiagramm noch im Trainingsmodus, zeigt der Profilbereich eine Benachrichtigung an. Die Meldung wird entfernt, wenn das Verhaltensdiagramm Daten für mindestens zwei Wochen gesammelt hat. Weitere Informationen zum Trainingsmodus finden Sie unter the section called "Trainingszeit für neue Verhaltensdiagramme".</p>

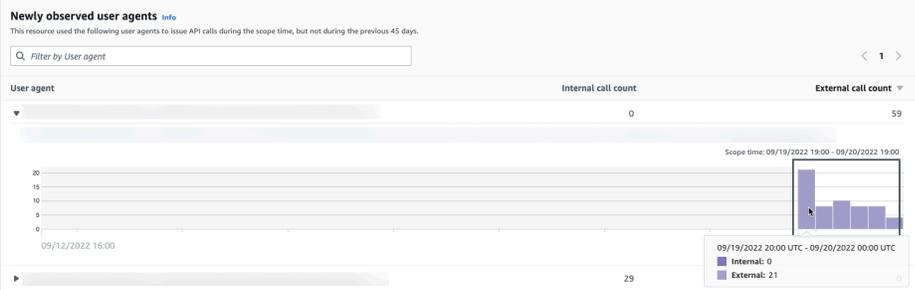
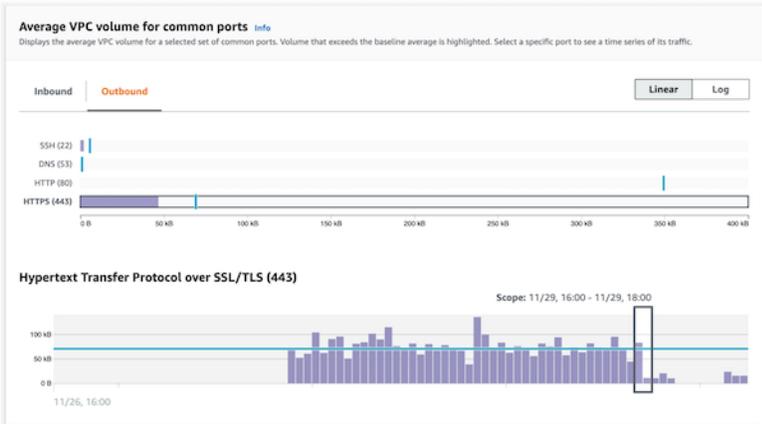
Arten von Visualisierungen in Profilbereichen

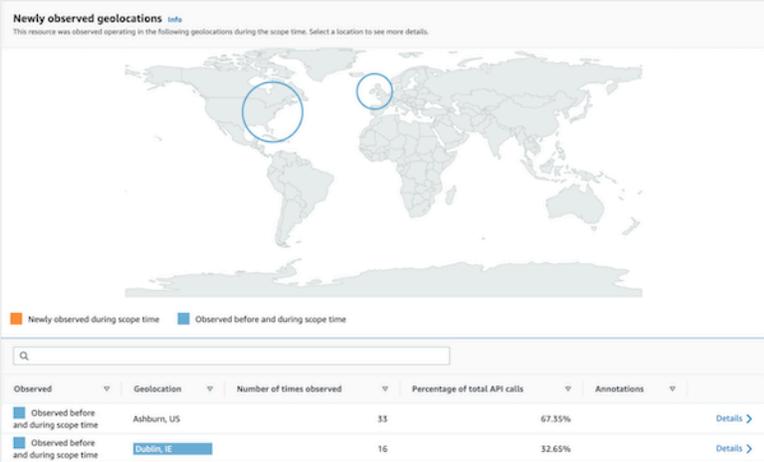
Der Inhalt des Profilbereichs kann eine der folgenden Formen annehmen.

Art der Visualisierung	Beschreibung
Schlüssel-Wert-Paare	<p>Die einfachste Art der Visualisierung ist eine Reihe von Schlüssel-Wert-Paaren.</p> <p>Ein Feld mit Befund- oder Entitätsinformationen ist das gängigste Beispiel für einen Schlüssel-Wert-Paar-Bereich.</p>

Art der Visualisierung	Beschreibung															
	 <p>Role details Info</p> <table border="1"> <tr> <td>AWS role</td> <td>Principal ID</td> <td>AWS account</td> </tr> <tr> <td>Created by</td> <td>Created date</td> <td>Last observed</td> </tr> <tr> <td>-</td> <td>-</td> <td>09/20/2022 16:46 UTC</td> </tr> <tr> <td>Role description</td> <td></td> <td></td> </tr> <tr> <td>-</td> <td></td> <td></td> </tr> </table> <p>Schlüssel-Wert-Paare können auch verwendet werden, um zusätzliche Informationen zu anderen Bereichstypen hinzuzufügen.</p> <p>Wenn es sich bei einem Wert um einen Kennzeichner einer Entität handelt, können Sie in einem Bereich mit Schlüssel-Wert-Paaren zu ihrem Profil wechseln.</p>	AWS role	Principal ID	AWS account	Created by	Created date	Last observed	-	-	09/20/2022 16:46 UTC	Role description			-		
AWS role	Principal ID	AWS account														
Created by	Created date	Last observed														
-	-	09/20/2022 16:46 UTC														
Role description																
-																
Tabelle	<p>Eine Tabelle ist eine einfache mehrspaltige Liste von Elementen.</p>  <p>Observed IP address assignments based on VPC Flow These IP addresses were assigned to this EC2 instance and also had traffic with the instance</p> <p>Filter by IP CIDR</p> <table border="1"> <thead> <tr> <th>IP address</th> <th>First observed</th> <th>Last observed</th> </tr> </thead> <tbody> <tr> <td>10.101.0.119</td> <td>04/27/2021 15:19 UTC</td> <td>09/20/2022 17:45 UTC</td> </tr> </tbody> </table> <p>Sie können die Tabelle sortieren, filtern und durchblättern.</p> <p>Sie können die Anzahl der Einträge ändern, die auf jeder Seite angezeigt werden sollen. Siehe the section called “Einstellungen für Profilbereiche”.</p> <p>Wenn ein Wert in der Tabelle ein Bezeichner einer Entität ist, können Sie zu ihrem Profil wechseln.</p>	IP address	First observed	Last observed	10.101.0.119	04/27/2021 15:19 UTC	09/20/2022 17:45 UTC									
IP address	First observed	Last observed														
10.101.0.119	04/27/2021 15:19 UTC	09/20/2022 17:45 UTC														

Art der Visualisierung	Beschreibung
Zeitplan	<p>Eine Zeitleistenvisualisierung zeigt einen aggregierten Wert für definierte Intervalle im Zeitverlauf.</p>  <p>In der Zeitleiste wird der aktuelle Zeitbereich hervorgehoben und zusätzliche Peripheriezeit vor und nach der Gültigkeitsdauer berücksichtigt. Die Peripheriezeit bietet den Kontext für die Aktivität im Zeitbereich.</p> <p>Zeigen Sie mit der Maus auf ein Zeitintervall, um eine Übersicht der Daten für dieses Zeitintervall anzuzeigen.</p>

Art der Visualisierung	Beschreibung
Erweiterbare Tabelle	<p>Eine erweiterbare Tabelle kombiniert Tabellen und Zeitleisten.</p>  <p>Die Visualisierung beginnt als Tabelle.</p> <p>Sie können die Tabelle sortieren, filtern und durchblättern.</p> <p>Sie können die Anzahl der Einträge ändern, die auf jeder Seite angezeigt werden sollen. Siehe the section called “Einstellungen für Profilbereiche”.</p> <p>Sie können dann jede Zeile erweitern, um eine für diese Zeile spezifische Zeitleistenvisualisierung anzuzeigen.</p>
Balkendiagramm	<p>Ein Balkendiagramm zeigt Werte, die auf Gruppierungen basieren.</p> <p>Je nach Diagramm können Sie einen Balken auswählen, um eine Zeitleiste verwandter Aktivitäten anzuzeigen.</p> 

Art der Visualisierung	Beschreibung
Geolokalisierungsdiagramm	<p>In einem Geolokalisierungsdiagramm wird eine Karte angezeigt, die so gekennzeichnet ist, dass Daten anhand der geografischen Position hervorgehoben werden. Darauf kann eine Tabelle mit Details zu einzelnen Geolocations folgen.</p>  <p>Beachten Sie, dass Detective bei der Verarbeitung eingehender geografischer Daten die Breiten- und Längengrade auf eine einzige Dezimalstelle rundet.</p>

Weitere Hinweise zum Inhalt des Profilbereichs

Achten Sie beim Anzeigen des Inhalts eines Profilbereichs auf Folgendes:

Warnung vor ungefähren Zählwerten

Diese Warnung weist darauf hin, dass Elemente mit extrem niedriger Anzahl aufgrund der Menge der entsprechenden Daten nicht angezeigt werden.

Um eine absolut genaue Zählung zu gewährleisten, reduzieren Sie die Datenmenge. Der einfachste Weg, dies zu tun, besteht darin, die Dauer der Datenerhebung zu reduzieren. Siehe [the section called “Verwaltung des Zeitbereichs”](#).

Rundung für geografische Standorte

Detective rundet alle Breiten- und Längengrade auf eine einzige Dezimalstelle ab.

Änderungen an der Darstellung von API-Aufrufen durch Detective

Ab dem 14. Juli 2021 verfolgt Detective jeden Dienst, der API-Aufruf getätigt hat. Immer wenn Detective eine API-Methode anzeigt, wird auch der zugehörige Dienst angezeigt. In Profilbereichen, in denen Informationen zu API-Aufrufen angezeigt werden, sind die Aufrufe immer nach dem Dienst gruppiert. Für Daten, die Detective vor diesem Datum aufgenommen hat, wird der Dienstname als Unbekannter Dienst aufgeführt.

Ebenfalls ab dem 14. Juli 2021 wird in den Aktivitätsdetails für Konten und Rollen im Profilbereich Gesamtes API-Aufrufvolumen nicht mehr die AKID der Ressource angezeigt, die den Aufruf getätigt hat. Für Konten zeigt Detective die ID des Prinzipals (Benutzer oder Rolle) an, der den Aufruf getätigt hat. Für Rollen zeigt Detective die ID der Rollen-Sitzung an. Für Daten, die Detective vor dem 14. Juli 2021 aufgenommen hat, wird der Kennzeichner als Unbekannte Ressource aufgeführt.

Bei Profilbereichen, die eine Liste von API-Aufrufen anzeigen, wird in der zugehörigen Zeitleiste der Zeitraum hervorgehoben, in dem dieser Übergang stattgefunden hat. Das Highlight beginnt am 14. Juli 2021 und endet, wenn das Update vollständig in Detective propagiert wurde.

Festlegen der Einstellungen für einen Profilbereich

In der Detective-Konsole können Sie die Tabellenlänge und die Zeitstempelanzeige auf der Seite Einstellungen festlegen.

Einstellung der Tabellenlänge

Für Profilbereiche, die Tabellen oder erweiterbare Tabellen enthalten, können Sie die Anzahl der Zeilen konfigurieren, die auf jeder Seite angezeigt werden sollen.

Legen Sie Ihre Präferenz für die Anzahl der Einträge auf jeder Seite fest.

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Detective-Navigationsbereich unter Einstellungen die Option Präferenzen aus.
3. Klicken Sie auf der Seite Einstellungen unter Tabellenlänge auf Bearbeiten.
4. Wählen Sie die Anzahl der Tabellenzeilen aus, die Sie auf jeder Seite anzeigen möchten.
5. Wählen Sie Speichern.

Festlegen des Zeitstempelformats

Für Profilbereiche können Sie die Einstellung für das Zeitstempelformat konfigurieren, die auf alle Zeitstempel für jeden IAM-Benutzer oder jede IAM-Rolle in Detective angewendet wird.

Note

Die Voreinstellung für das Zeitstempelformat wird nicht auf das gesamte AWS Konto angewendet.

Legen Sie die Präferenz für den Zeitstempel fest.

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Detective-Navigationsbereich unter Einstellungen die Option Präferenzen aus.
3. Auf der Seite Einstellungen können Sie unter Zeitstempелеinstellungen die bevorzugte Anzeige für alle Zeitstempel anzeigen und ändern.
4. Standardmäßig ist das Zeitstempelformat auf UTC eingestellt. Klicken Sie auf Bearbeiten, um Ihre lokale Zeitzone auszuwählen.

Beispiel:

Example

UTC – 20.09.22 16:39 UTC

Lokal – 20.09.2022 9:39 (UTC-07:00)

5. Wählen Sie Speichern.

Von einem Profilbereich zu einer anderen Konsole wechseln

Für EC2-Instances, IAM-Benutzer und IAM-Rollen können Sie direkt vom Profilbereich mit den Details zur entsprechenden Konsole navigieren. Die in der Konsole verfügbaren Informationen können zusätzliche Informationen für Ihre Untersuchung liefern.

Im Profilbereich mit den EC2-Instance-Details ist die EC2-Instance-ID mit der Amazon-EC2-Konsole verknüpft.

Im Profilbereich mit den Benutzerdetails ist der Benutzername mit der IAM-Konsole verknüpft.

Im Profilbereich Rollendetails ist der Rollename mit der IAM-Konsole verknüpft.

Von einem Profilbereich zu einem anderen Entitätsprofil wechseln

Wenn ein Profilbereich eine Kennung einer anderen Entität enthält, handelt es sich normalerweise um einen Link zu diesem Entitätsprofil. Ausnahmen sind die Links zu den Amazon-EC2- und IAM-Konsolen auf der EC2-Instance, IAM-Benutzer und IAM-Rollenprofile. Siehe [the section called “Zu einer anderen Konsole wechseln”](#).

Beispielsweise können Sie anhand einer Liste von IP-Adressen möglicherweise das Profil für eine bestimmte IP-Adresse anzeigen. Auf diese Weise können Sie sehen, ob weitere Informationen verfügbar sind, die Ihnen beim Abschluss Ihrer Untersuchung helfen könnten.

Erkunden von Aktivitätsdetails in einem Profilbereich

Während einer Untersuchung möchten Sie möglicherweise das Aktivitätsmuster einer Entität genauer untersuchen.

In den folgenden Profilbereichen können Sie eine Übersicht der Aktivitätsdetails anzeigen:

- Gesamtes API-Aufrufvolumen, mit Ausnahme des Profilbereichs im Benutzer-Agenten-Profil
- Neu beobachtete Geolocations
- Gesamtes VPC-Datendurchflussvolumen
- VPC-Datendurchflussvolumen zur und von der findenden IP-Adresse für Erkenntnisse, die mit einer einzelnen IP-Adresse verknüpft sind
- Details zum Container
- VPC-Datendurchflussvolumen für Cluster
- Allgemeine Kubernetes-API-Aktivität

Die Aktivitätsdetails können die folgenden Arten von Fragen beantworten:

- Welche IP-Adressen wurden verwendet?
- Wo befanden sich diese IP-Adressen?
- Welche API-Aufrufe haben die einzelnen IP-Adressen getätigt und von welchen Diensten aus haben sie diese Aufrufe getätigt?
- Welche Prinzipale oder Access Key Identifier (AKIDs) wurden für die Aufrufe verwendet?
- Welche Ressourcen wurden für diese Aufrufe verwendet?

- Wie viele Aufrufe wurden getätigt? Wie viele waren erfolgreich und sind gescheitert?
- Welches Volumen an VPC-Datendurchfluss-Protokolldaten wurde an oder von jeder IP-Adresse gesendet?
- Welche Container waren für einen bestimmten Cluster, ein bestimmtes Image oder einen Pod aktiv?

Themen

- [Aktivitätsdetails für das gesamte API-Aufrufvolumen](#)
- [Aktivitätsdetails für eine Geolokalisierung](#)
- [Aktivitätsdetails für das gesamte VPC-Datendurchflussvolumen](#)
- [Allgemeine Kubernetes-API-Aktivität mit Beteiligung des EKS-Clusters](#)

Aktivitätsdetails für das gesamte API-Aufrufvolumen

Die Aktivitätsdetails für das API-Aufrufvolumen insgesamt zeigen die API-Aufrufe an, die in einem ausgewählten Zeitraum ausgegeben wurden.

Um die Aktivitätsdetails für ein einzelnes Zeitintervall anzuzeigen, wählen Sie das Zeitintervall im Diagramm aus.

Um die Aktivitätsdetails für den aktuellen Zeitbereich anzuzeigen, wählen Sie Details für den Zeitbereich anzeigen aus.

Beachten Sie, dass Detective ab dem 14. Juli 2021 damit begann, den Dienstnamen für API-Aufrufe zu speichern und anzuzeigen. Dieses Datum ist auf der Zeitleiste des Profilbereichs hervorgehoben. Für Aktivitäten, die vor diesem Datum stattfinden, lautet der Dienstname Unbekannter Dienst.

Inhalt der Aktivitätsdetails (Benutzer, Rollen, Konten, Rollensitzungen, EC2-Instances, S3-Buckets)

Für IAM-Benutzer, IAM-Rollen, Konten, Rollensitzungen, EC2-Instances und S3-Buckets enthalten die Aktivitätsdetails die folgenden Informationen:

- Jede Registerkarte enthält Informationen zu den API-Aufrufen, die während des ausgewählten Zeitraums ausgegeben wurden.

Bei S3-Buckets spiegeln die Informationen API-Aufrufe wider, die an den S3-Bucket getätigt wurden.

Die API-Aufrufe sind nach den Diensten gruppiert, die sie aufgerufen haben. Für S3-Buckets ist der Dienst immer Amazon S3. Wenn Detective den Dienst nicht ermitteln kann, der einen Aufruf getätigt hat, wird der Aufruf unter Unbekannter Dienst aufgeführt.

- Für jeden Eintrag zeigen die Aktivitätsdetails die Anzahl der erfolgreichen und fehlgeschlagenen Aufrufe. Auf der Registerkarte Beobachtete IP-Adressen wird auch der Standort jeder IP-Adresse angezeigt.
- Jeder Eintrag enthält Informationen darüber, wer die Aufrufe getätigt hat. Bei Konten identifizieren die Aktivitätsdetails die Benutzer oder Rollen. Bei Rollen identifizieren die Aktivitätsdetails die Rollensitzungen. Bei Benutzern und Rollensitzungen identifizieren die Aktivitätsdetails die Access Key Identifier (AKIDs).

Beachten Sie, dass ab dem 14. Juli 2021 in den Aktivitätsdetails für Kontoprofile Benutzer oder Rollen statt AKIDs angezeigt werden. Bei Rollenprofilen werden in den Aktivitätsdetails Rollensitzungen statt AKIDs angezeigt. Bei Aktivitäten, die vor dem 14. Juli 2021 stattfinden, wird der Aufrufer als Unbekannte Ressource aufgeführt.

Die Aktivitätsdetails enthalten die folgenden Tabs:

Beobachtete IP-Adressen

Zeigt zunächst die Liste der IP-Adressen an, die für API-Aufrufe verwendet werden.

Sie können jede IP-Adresse erweitern, um die Liste der API-Aufrufe anzuzeigen, die von dieser IP-Adresse aus getätigt wurden. Die API-Aufrufe sind nach den Diensten gruppiert, die sie aufgerufen haben. Für S3-Buckets ist der Dienst immer Amazon S3. Wenn Detective den Dienst nicht ermitteln kann, der einen Aufruf getätigt hat, wird der Aufruf unter Unbekannter Dienst aufgeführt.

Sie können dann jeden API-Aufruf erweitern, um die Liste der Aufrufer von dieser IP-Adresse anzuzeigen. Je nach Profil kann es sich bei dem Aufrufer um einen Benutzer, eine Rolle, eine Rollensitzung oder eine AKID handeln.

Showing activity: 07/08/2021, 00:00 UTC - 07/08/2021, 04:00 UTC Edit

Observed IP addresses | **API method by service** | Resource

Filter by IP CIDR, Service name, API Method name, or Resource string

IP address	Successful calls	Failed calls	Location
[redacted]	421	311	-
▶ s3	316	311	
▶ config	61	0	
▼ kms	15	0	
▼ DescribeKey	14	0	
[redacted] Role session ([redacted])	14	0	
▶ ListKeys	1	0	
▶ rds	7	0	
▶ ec2	4	0	
▶ autoscaling	3	0	
▶ secretsmanager	2	0	
▶ guardduty	2	0	
▶ es	2	0	

API-Methode nach Dienst

Zeigt zunächst die Liste der API-Aufrufe an, die ausgegeben wurden. Die API-Aufrufe sind nach den Diensten gruppiert, die die Aufrufe ausgegeben haben. Für S3-Buckets ist der Dienst immer Amazon S3. Wenn Detective den Dienst nicht ermitteln kann, der einen Aufruf getätigt hat, wird der Aufruf unter Unbekannter Dienst aufgeführt.

Sie können jede API-Methode erweitern, um die Liste der IP-Adressen anzuzeigen, von denen aus die Aufrufe getätigt wurden.

Sie können dann jede IP-Adresse erweitern, um die Liste der AKIDs anzuzeigen, die den API-Aufruf von dieser IP-Adresse aus ausgeführt haben.

Showing activity: 07/08/2021, 00:00 UTC - 07/08/2021, 04:00 UTC Edit

Observed IP addresses | **API method by service** | Resource

Filter by IP CIDR, Service name, API Method name, or Resource string

API method	Successful calls	Failed calls
▶ s3	316	311
▶ config	61	0
▼ kms	15	0
▼ DescribeKey	14	0
[redacted]	14	0
[redacted] Role session ([redacted])	14	0
▶ ListKeys	1	0
▶ rds	7	0
▶ ec2	4	0
▶ autoscaling	3	0

Ressourcen- oder Zugriffsschlüssel-ID

Zeigt zunächst die Liste der Benutzer, Rollen, Rollensitzungen oder AKIDs an, die für API-Aufrufe verwendet wurden.

Sie können jeden Aufrufer erweitern, um die Liste der IP-Adressen anzuzeigen, von denen der Aufrufer API-Aufrufe ausgegeben hat.

Sie können dann jede IP-Adresse erweitern, um die Liste der API-Aufrufe anzuzeigen, die von diesem Aufrufer von dieser IP-Adresse aus getätigt wurden. Die API-Aufrufe sind nach den Diensten gruppiert, die die Aufrufe ausgegeben haben. Für S3-Buckets ist der Dienst immer Amazon S3. Wenn Detective den Dienst nicht ermitteln kann, der einen Aufruf getätigt hat, wird der Aufruf unter Unbekannter Dienst aufgeführt.

Resource	Successful calls	Failed calls
Role session	322	310
Role session	91	0
Role session	91	0
config	61	0
kms	15	0
DescribeKey	14	0
ListKeys	1	0
ec2	3	0
secretsmanager	2	0
guardduty	2	0
...

Inhalt der Aktivitätsdetails (IP-Adressen)

Bei IP-Adressen enthalten die Aktivitätsdetails die folgenden Informationen:

- Jede Registerkarte enthält Informationen zu den API-Aufrufen, die während des ausgewählten Zeitraums ausgegeben wurden. Die API-Aufrufe sind nach den Diensten gruppiert, die die Aufrufe ausgegeben haben. Wenn Detective den Dienst nicht ermitteln kann, der einen Aufruf getätigt hat, wird der Aufruf unter Unbekannter Dienst aufgeführt.
- Für jeden Eintrag zeigen die Aktivitätsdetails die Anzahl der erfolgreichen und fehlgeschlagenen Aufrufe.

Die Aktivitätsdetails enthalten die folgenden Tabs:

Ressource

Zeigt zunächst die Liste der Ressourcen an, die API-Aufrufe von der IP-Adresse aus ausgegeben haben.

Für jede Ressource enthält die Liste den Namen, den Typ und das AWS -Konto der Ressource.

Sie können jede Ressource erweitern, um die Liste der API-Aufrufe anzuzeigen, die die Ressource über die IP-Adresse ausgegeben hat. Die API-Aufrufe sind nach den Diensten gruppiert, die die Aufrufe ausgegeben haben. Wenn Detective den Dienst nicht ermitteln kann, der einen Aufruf getätigt hat, wird der Aufruf unter Unbekannter Dienst aufgeführt.

Showing activity: 07/08/2021, 00:00 UTC - 07/08/2021, 04:00 UTC Edit

Resource | API method by service

Filter by Resource string, Service name or API Method name

Resource	Successful calls	Failed calls	Account ID
<ul style="list-style-type: none"> <ul style="list-style-type: none"> DescribeComplianceByConfigRule PutEvaluations SelectResourceConfig DescribeDeliveryChannelStatus DescribeConfigurationRecorderSta... DescribeConfigurationRecorders ec2 shield waf-regional 	3,520	0	
config	1,754	0	
	1,408	0	
	244	0	
	78	0	
	8	0	
	8	0	
	8	0	
	1,690	0	
	50	0	
	26	0	
	1,715	0	
	504	480	

API-Methode nach Dienst

Zeigt zunächst die Liste der API-Aufrufe an, die ausgegeben wurden. Die API-Aufrufe sind nach den Diensten gruppiert, die die Aufrufe ausgegeben haben. Wenn Detective den Dienst nicht ermitteln kann, der einen Aufruf getätigt hat, wird der Aufruf unter Unbekannter Dienst aufgeführt.

Sie können jeden API-Aufruf erweitern, um die Liste der Ressourcen anzuzeigen, die im ausgewählten Zeitraum den API-Aufruf von der IP-Adresse aus getätigt haben.

Showing activity: 07/08/2021, 00:00 UTC - 07/08/2021, 04:00 UTC Edit

Resource | API method by service

Filter by Resource string, Service name or API Method name

API method	Successful calls	Failed calls
config	3,787	0
ec2	2,538	0
s3	1,269	1,016
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ListCommands SendCommand 	481	16
	392	0
	222	0
	170	0
	89	16
logs	165	0
sts	149	0
iam	149	12

Sortierung der Aktivitätsdetails

Sie können die Aktivitätsdetails nach jeder beliebigen Listenspalte sortieren.

Wenn Sie anhand der ersten Spalte sortieren, wird nur die Liste der obersten Ebene sortiert. Die Listen auf niedrigerer Ebene sind immer nach der Anzahl der erfolgreichen API-Aufrufe sortiert.

Filterung der Aktivitätsdetails

Sie können die Filteroptionen verwenden, um sich auf bestimmte Teilmengen oder Aspekte der Aktivität zu konzentrieren, die in den Aktivitätsdetails dargestellt sind.

Auf allen Registerkarten können Sie die Liste nach beliebigen Werten in der ersten Spalte filtern.

So fügen Sie einen Filter hinzu

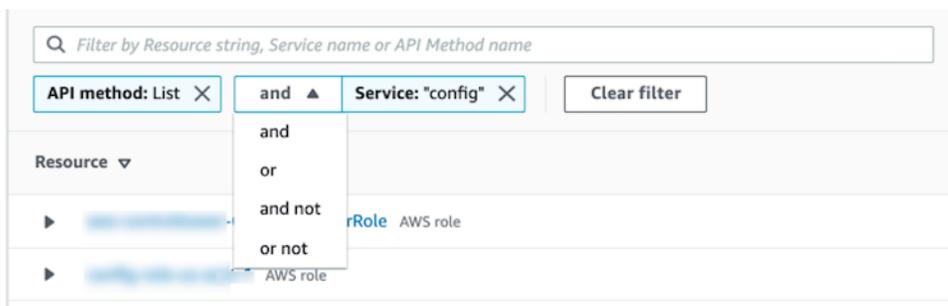
1. Wählen Sie das Filterfeld.
2. Wählen Sie unter Eigenschaften die Eigenschaft aus, die für die Filterung verwendet werden soll.
3. Geben Sie den Wert an, der für die Filterung verwendet werden soll. Der Filter unterstützt Teilwerte. Wenn Sie beispielsweise nach einer API-Methode filtern und nach **Instance** filtern, enthalten die Ergebnisse alle API-Operationen, deren Name das Wort Instance enthält. Also sowohl ListInstanceAssociations als auch UpdateInstanceInformation würden passen.

Für Dienstnamen, API-Methoden und IP-Adressen können Sie entweder einen Wert angeben oder einen integrierten Filter auswählen.

Wählen Sie für Common API-Teilstrings die Teilzeichenfolge aus, die den Vorgangstyp darstellt, z. B. List, Create oder Delete. Jeder API-Methodenname beginnt mit dem Operationstyp.

Für CIDR-Muster können Sie wählen, ob Sie nur öffentliche IP-Adressen, private IP-Adressen oder IP-Adressen einbeziehen möchten, die einem bestimmten CIDR-Muster entsprechen.

4. Wenn Sie mehrere Filter haben, wählen Sie eine boolesche Option, um festzulegen, wie diese Filter miteinander verbunden sind.



5. Um einen Filter zu entfernen, wählen Sie das Symbol x in der rechten oberen Ecke.

6. Um alle Filter zu löschen, wählen Sie Filter löschen aus.

Auswählen des Zeitbereichs für die Aktivitätsdetails

Wenn Sie die Aktivitätsdetails zum ersten Mal anzeigen, entspricht der Zeitraum entweder dem Zeitbereich oder einem ausgewählten Zeitintervall. Sie können den Zeitraum für die Aktivitätsdetails ändern.

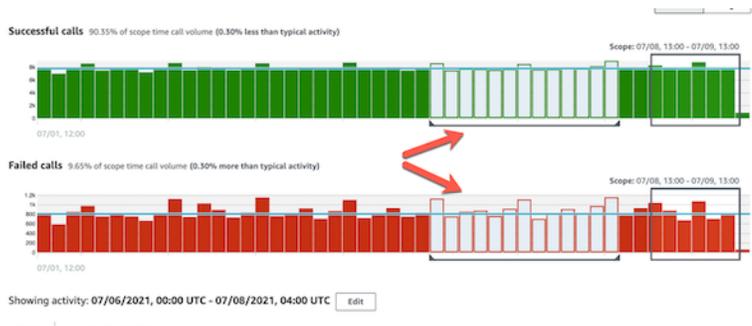
So ändern Sie einen Zeitraum für die Aktivitätsdetails

1. Wählen Sie Bearbeiten aus.
2. Wählen Sie unter Zeitfenster bearbeiten die zu verwendende Start- und Endzeit aus.

Um das Zeitfenster auf die standardmäßige Gültigkeitsdauer für das Profil festzulegen, wählen Sie Auf Standardzeit für den Geltungsbereich festlegen.

3. Wählen Sie Zeitfenster aktualisieren.

Der Zeitraum für die Aktivitätsdetails ist in den Diagrammen des Profilbereichs hervorgehoben.



Abfragen von unformatierten Protokollen

Amazon Detective ist in Amazon Security Lake integriert, was bedeutet, dass Sie die von Security Lake gespeicherten Rohprotokolldaten abfragen und abrufen können. Weitere Informationen zu dieser Integration finden Sie unter [Integration mit Amazon Security Lake](#).

Mithilfe dieser Integration können Sie Protokolle und Ereignisse aus den folgenden Quellen sammeln und abfragen, die Security Lake nativ unterstützt.

- AWS CloudTrail Verwaltungsereignisse
- Amazon Virtual Private Cloud (Amazon VPC)-Datendurchflussprotokolle

Note

Für die Abfrage von Rohdatenprotokollen in Detective fallen keine zusätzlichen Gebühren an. Nutzungsgebühren für andere AWS Services, einschließlich Amazon Athena, fallen weiterhin zu den veröffentlichten Tarifen an.

So fragen Sie Rohprotokolle ab

1. Wählen Sie Details für den Zeitbereich anzeigen aus.
2. Von hier aus können Sie mit der Abfrage von Rohprotokollen beginnen.
3. In der Vorschautabelle für Rohprotokolle können Sie die Protokolle und Ereignisse anzeigen, die durch Abfragen von Daten aus Security Lake abgerufen wurden. Weitere Informationen zu den unbearbeiteten Ereignisprotokollen finden Sie in den in Amazon Athena angezeigten Daten.

In der Tabelle „Rohdatenprotokolle abfragen“ können Sie die Abfrageanfrage stornieren, Ergebnisse in Amazon Athena anzeigen und Ergebnisse als Datei mit kommagetrennten Werten (.csv) herunterladen.

Wenn Sie Protokolle in Detective sehen, die Abfrage aber keine Ergebnisse lieferte, kann das aus den folgenden Gründen passieren.

- Rohprotokolle werden möglicherweise in Detective verfügbar, bevor sie in den Security-Lake-Protokolltabellen angezeigt werden. Bitte versuchen Sie es später erneut.
- In Security Lake fehlen möglicherweise Protokolle. Wenn Sie über einen längeren Zeitraum gewartet haben, deutet dies darauf hin, dass Protokolle in Security Lake fehlen. Wenden Sie sich an Ihren Security-Lake-Administrator, um das Problem zu beheben.

Aktivitätsdetails für eine Geolokalisierung

Die Aktivitätsdetails für Neu beobachtete Geolocations zeigen die API-Aufrufe, die während des Gültigkeitszeitraums von einer Geolocation aus getätigt wurden. Die API-Aufrufe umfassen alle Aufrufe, die von der Geolocation aus getätigt wurden. Sie sind nicht auf Aufrufe beschränkt, bei denen die Such- oder Profilentität verwendet wurde. Bei S3-Buckets handelt es sich bei den Aktivitätsaufrufen um API-Aufrufe an den S3-Bucket.

Detective bestimmt den Standort von Anfragen mithilfe von MaxMind GeolP-Datenbanken. MaxMind meldet eine sehr hohe Genauigkeit ihrer Daten auf Landesebene, obwohl die Genauigkeit je nach Faktoren wie Land und Art des geistigen Eigentums variiert. Weitere Informationen MaxMind dazu finden Sie unter [MaxMind IP-Geolokalisierung](#). Wenn Sie der Meinung sind, dass einige der GeolP-Daten falsch sind, können Sie unter [MaxMind Correct GeolP2](#) Data eine Korrekturanfrage an Maxmind stellen.

Die API-Aufrufe sind nach den Diensten gruppiert, die die Aufrufe ausgegeben haben. Für S3-Buckets ist der Dienst immer Amazon S3. Wenn Detective den Dienst nicht ermitteln kann, der einen Aufruf getätigt hat, wird der Aufruf unter Unbekannter Dienst aufgeführt.

Um die Aktivitätsdetails anzuzeigen, führen Sie einen der folgenden Schritte aus:

- Wählen Sie auf der Karte eine Geolocation aus.
- Wählen Sie in der Liste Details für eine Geolocation aus.

Die Aktivitätsdetails ersetzen die Geolocation-Liste. Um zur Geolocation-Liste zurückzukehren, wählen Sie Zurück zu allen Ergebnissen.

Beachten Sie, dass Detective ab dem 14. Juli 2021 damit begann, den Dienstnamen für API-Aufrufe zu speichern und anzuzeigen. Für Aktivitäten, die vor diesem Datum stattfinden, lautet der Dienstname Unbekannter Dienst.

Inhalt der Aktivitätsdetails

Jede Registerkarte enthält Informationen zu allen API-Aufrufen, die während des Gültigkeitszeitraums von der Geolocation aus getätigt wurden.

Für jede IP-Adresse, Ressource und API-Methode zeigt die Liste die Anzahl der erfolgreichen und fehlgeschlagenen API-Aufrufe.

Die Aktivitätsdetails enthalten die folgenden Tabs:

Beobachtete IP-Adressen

Zeigt zunächst die Liste der IP-Adressen an, die für API-Aufrufe von der ausgewählten Geolocation aus verwendet wurden.

Sie können jede IP-Adresse erweitern, um die Ressourcen anzuzeigen, die API-Aufrufe von dieser IP-Adresse aus ausgegeben haben. In der Liste wird der Ressourcename angezeigt. Um die Prinzipal-ID zu sehen, bewegen Sie den Mauszeiger über den Namen.

Anschließend können Sie jede Ressource erweitern, um die spezifischen API-Aufrufe anzuzeigen, die von dieser Ressource von dieser IP-Adresse aus ausgegeben wurden. Die API-Aufrufe sind nach den Diensten gruppiert, die die Aufrufe ausgegeben haben. Für S3-Buckets ist der Dienst immer Amazon S3. Wenn Detective den Dienst nicht ermitteln kann, der einen Aufruf getätigt hat, wird der Aufruf unter Unbekannter Dienst aufgeführt.

IP address	Successful calls	Failed calls
192.168.1.1	27,564	2,453
aws-logs-523123456789.us-east-1.amazonaws.com AWS role (arn:aws:iam::123456789012:role/lambda-logs-role)	27,564	2,453
ssm	25,111	0
UpdateInstanceInformation	13,066	0
ListInstanceAssociations	6,482	0
PutInventory	2,544	0
GetDeployablePatchSnapshotForIns...	2,453	0
UpdateInstanceAssociationStatus	466	0
PutComplianceItems	98	0
GetDocument	2	0
sts	2,453	0
s3	0	2,453
192.168.1.2	24,635	1,512
192.168.1.3	24,632	1,511

Ressource

Zeigt zunächst die Liste der Ressourcen an, die API-Aufrufe von der ausgewählten Geolocation aus getätigt haben. In der Liste wird der Ressourcename angezeigt. Um die Prinzipal-ID zu sehen, machen Sie eine Pause beim Namen. Für jede Ressource werden auf der Registerkarte Ressource auch die zugehörigen AWS-Konto angezeigt.

Sie können jeden Benutzer oder jede Rolle erweitern, um die Liste der API-Aufrufe anzuzeigen, die von dieser Ressource ausgegeben wurden. Die API-Aufrufe sind nach den Diensten gruppiert, die die Aufrufe ausgegeben haben. Für S3-Buckets ist der Dienst immer Amazon S3. Wenn Detective den Dienst nicht ermitteln kann, der einen Aufruf getätigt hat, wird der Aufruf unter Unbekannter Dienst aufgeführt.

Sie können dann jeden API-Aufruf erweitern, um die Liste der IP-Adressen anzuzeigen, von denen die Ressource den API-Aufruf ausgeführt hat.

Ashburn, US from 05/14/2021 - 06/28/2021

Observed IP addresses **Resource**

Filter by IP CIDR, API Method name, or Resource string

Resource	Successful calls	Failed calls	Account ID
▶ [redacted] AWS role	189,097	17	[redacted]
▼ [redacted] AWS role	49,267	3,023	[redacted]
▼ ssm	46,254	0	
▼ UpdateInstanceInformation	25,932	0	
▶ [redacted]	12,968	0	
▶ [redacted]	12,964	0	
▶ ListInstanceAssociations	12,964	0	
▶ PutInventory	3,194	0	
▶ GetDeployablePatchSnapshotForIns...	3,011	0	
▶ UpdateInstanceAssociationStatus	949	0	
▶ PutComplianceItems	199	0	
▶ GetDocument	5	0	
▶ sts	3,013	0	
▶ s3	0	3,023	

Sortierung der Aktivitätsdetails

Sie können die Aktivitätsdetails nach jeder beliebigen Listenspalte sortieren.

Wenn Sie anhand der ersten Spalte sortieren, wird nur die Liste der obersten Ebene sortiert. Die Listen auf niedrigerer Ebene sind immer nach der Anzahl der erfolgreichen API-Aufrufe sortiert.

Filterung der Aktivitätsdetails

Sie können die Filteroptionen verwenden, um sich auf bestimmte Teilmengen oder Aspekte der Aktivität zu konzentrieren, die in den Aktivitätsdetails dargestellt sind.

Auf allen Registerkarten können Sie die Liste nach beliebigen Werten in der ersten Spalte filtern.

So fügen Sie einen Filter hinzu

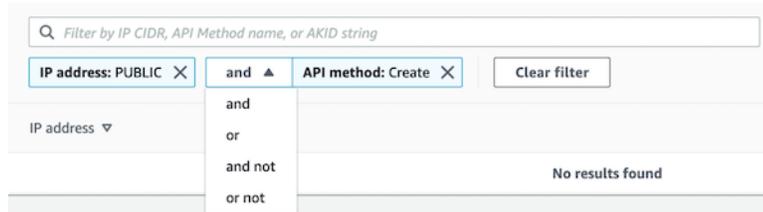
1. Wählen Sie das Filterfeld.
2. Wählen Sie unter Eigenschaften die Eigenschaft aus, die für die Filterung verwendet werden soll.
3. Geben Sie den Wert an, der für die Filterung verwendet werden soll. Der Filter unterstützt Teilwerte. Wenn Sie beispielsweise nach einer API-Methode filtern und nach **Instance** filtern, enthalten die Ergebnisse alle API-Operationen, deren Name das Wort Instance enthält. Also sowohl ListInstanceAssociations als auch UpdateInstanceInformation würden passen.

Für Dienstnamen, API-Methoden und IP-Adressen können Sie entweder einen Wert angeben oder einen integrierten Filter auswählen.

Wählen Sie für Common API-Teilstrings die Teilzeichenfolge aus, die den Vorgangstyp darstellt, z. B. List, Create oder Delete. Jeder API-Methodenname beginnt mit dem Operationstyp.

Für CIDR-Muster können Sie wählen, ob Sie nur öffentliche IP-Adressen, private IP-Adressen oder IP-Adressen einbeziehen möchten, die einem bestimmten CIDR-Muster entsprechen.

4. Wenn Sie mehrere Filter haben, wählen Sie eine boolesche Option, um festzulegen, wie diese Filter miteinander verbunden sind.



5. Um einen Filter zu entfernen, wählen Sie das Symbol x in der rechten oberen Ecke.
6. Um alle Filter zu löschen, wählen Sie Filter löschen aus.

Aktivitätsdetails für das gesamte VPC-Datendurchflussvolumen

Für eine EC2-Instance zeigen die Aktivitätsdetails für das Gesamte VPC-Datendurchflussvolumen die Interaktionen zwischen der EC2-Instance und IP-Adressen während eines ausgewählten Zeitraums.

Für einen Kubernetes-Pod zeigt Gesamtes VPC-Datendurchflussvolumen das Gesamtvolumen der Bytes an, die in die zugewiesene IP-Adresse des Kubernetes-Pods für alle Ziel-IP-Adressen ein- und ausgehen. Die IP-Adresse des Kubernetes-Pods ist nicht eindeutig, wenn `hostNetwork: true`. In diesem Fall zeigt der Bereich den Datenverkehr zu anderen Pods mit derselben Konfiguration und dem Knoten, der sie hostet.

Bei einer IP-Adresse zeigen die Aktivitätsdetails für das Gesamte VPC-Datendurchflussvolumen die Interaktionen zwischen der IP-Adresse und EC2-Instances während eines ausgewählten Zeitraums.

Um die Aktivitätsdetails für ein einzelnes Zeitintervall anzuzeigen, wählen Sie das Zeitintervall im Diagramm aus.

Um die Aktivitätsdetails für den aktuellen Zeitbereich anzuzeigen, wählen Sie Details für den Zeitbereich anzeigen aus.

Inhalt der Aktivitätsdetails

Der Inhalt spiegelt die Aktivität im ausgewählten Zeitraum wider.

Bei einer EC2-Instance enthalten die Aktivitätsdetails einen Eintrag für jede eindeutige Kombination aus IP-Adresse, lokalem Port, Remote-Port, Protokoll und Richtung.

Bei einer IP-Adresse enthalten die Aktivitätsdetails einen Eintrag für jede eindeutige Kombination aus EC2-Instance, lokalem Port, Remote-Port, Protokoll und Richtung.

Jeder Eintrag zeigt das Volumen des eingehenden Datenverkehrs, das Volumen des ausgehenden Datenverkehrs und ob die Zugriffsanfrage akzeptiert oder abgelehnt wurde. Bei der Suche nach Profilen gibt die Spalte Anmerkungen an, wann eine IP-Adresse mit der aktuellen Erkenntnis zusammenhängt.

Showing activity: 02/17/2021, 20:00 UTC - 02/18/2021, 00:00 UTC [Edit](#) Overall traffic

Q Filter < 1 2 3 4 5 6 7 ... 343 >

<input type="checkbox"/>	IP address	Local port	Remote port	Inbound traffic	Outbound traffic	Protocol	Directionality	Accept / Reject	Annotations
<input type="checkbox"/>	10.0.0.1	-	4444	596 B	9.45 kB	TCP	Outbound	Accept	From Finding
<input type="checkbox"/>	10.0.0.1	-	4444	596 B	23.3 kB	TCP	Outbound	Accept	From Finding
<input type="checkbox"/>	10.0.0.1	-	4444	258 B	9.09 kB	TCP	Outbound	Accept	From Finding
<input type="checkbox"/>	10.0.0.1	-	4444	216 B	5.93 kB	TCP	Outbound	Accept	From Finding
<input type="checkbox"/>	10.0.0.1	-	4444	216 B	6.07 kB	TCP	Outbound	Accept	From Finding
<input type="checkbox"/>	10.0.0.1	-	4444	164 B	10.8 kB	TCP	Outbound	Accept	From Finding
<input type="checkbox"/>	10.0.0.1	-	4444	164 B	8.77 kB	TCP	Outbound	Accept	From Finding
<input type="checkbox"/>	10.0.0.1	22	2264	7.75 MB	13.3 MB	TCP	Unknown	Accept	
<input type="checkbox"/>	10.0.0.1	-	53	2.59 MB	2.08 MB	UDP	Unknown	Accept	

Sortierung der Aktivitätsdetails

Sie können die Aktivitätsdetails nach einer beliebigen Spalte in der Tabelle sortieren.

Standardmäßig werden die Aktivitätsdetails zuerst nach den Anmerkungen und dann nach dem eingehenden Verkehr sortiert.

Filterung der Aktivitätsdetails

Um sich auf eine bestimmte Aktivität zu konzentrieren, können Sie die Aktivitätsdetails nach den folgenden Werten filtern:

- IP-Adresse oder EC2-Instance
- Lokaler oder Remote-Port
- Richtung
- Protokoll
- Ob die Anfrage akzeptiert oder abgelehnt wurde

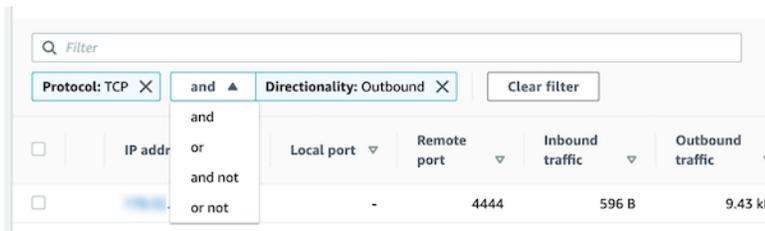
So fügen Sie Filter hinzu und entfernen sie

1. Wählen Sie das Filterfeld.
2. Wählen Sie unter Eigenschaften die Eigenschaft aus, die für die Filterung verwendet werden soll.
3. Geben Sie den Wert an, der für die Filterung verwendet werden soll. Der Filter unterstützt Teilwerte.

Um nach IP-Adresse zu filtern, können Sie entweder einen Wert angeben oder einen integrierten Filter auswählen.

Für CIDR-Muster können Sie wählen, ob Sie nur öffentliche IP-Adressen, private IP-Adressen oder IP-Adressen einbeziehen möchten, die einem bestimmten CIDR-Muster entsprechen.

4. Wenn Sie mehrere Filter haben, wählen Sie eine boolesche Option, um festzulegen, wie diese Filter miteinander verbunden sind.



5. Um einen Filter zu entfernen, wählen Sie das Symbol x in der rechten oberen Ecke.
6. Um alle Filter zu löschen, wählen Sie Filter löschen aus.

Auswählen des Zeitbereichs für die Aktivitätsdetails

Wenn Sie die Aktivitätsdetails zum ersten Mal anzeigen, entspricht der Zeitraum entweder dem Zeitbereich oder einem ausgewählten Zeitintervall. Sie können den Zeitraum für die Aktivitätsdetails ändern.

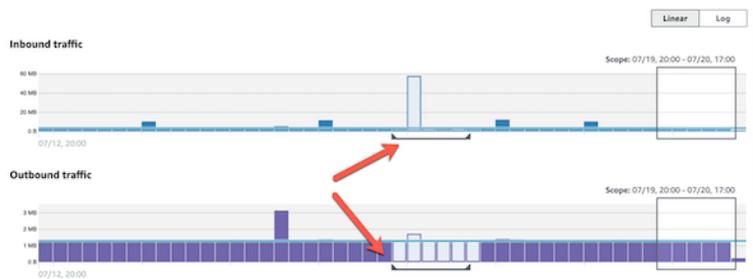
So ändern Sie einen Zeitraum für die Aktivitätsdetails

1. Wählen Sie Bearbeiten aus.
2. Wählen Sie unter Zeitfenster bearbeiten die zu verwendende Start- und Endzeit aus.

Um das Zeitfenster auf die standardmäßige Gültigkeitsdauer für das Profil festzulegen, wählen Sie Auf Standardzeit für den Geltungsbereich festlegen.

3. Wählen Sie Zeitfenster aktualisieren.

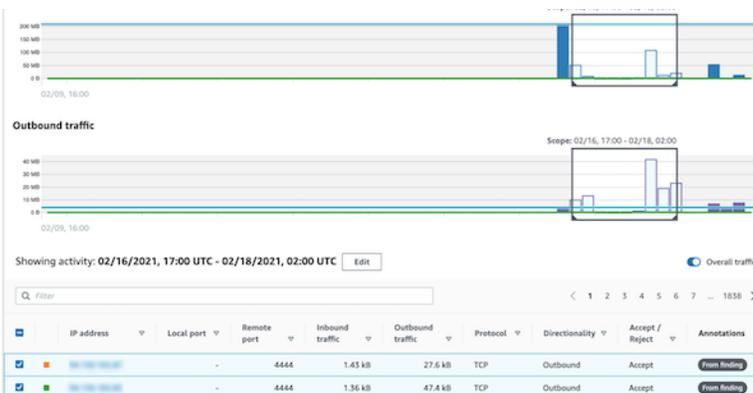
Der Zeitraum für die Aktivitätsdetails ist in den Diagrammen des Profilbereichs hervorgehoben.



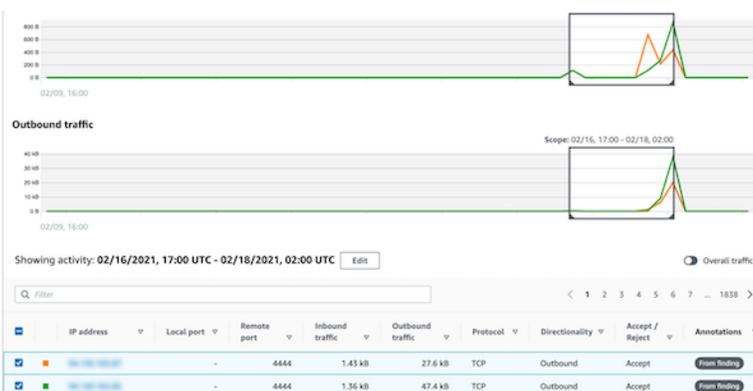
Anzeige des Verkehrsaufkommens für ausgewählte Zeilen

Wenn Sie Zeilen identifizieren, die für Sie von Interesse sind, können Sie in den Hauptdiagrammen das Verkehrsaufkommen für diese Zeilen im Zeitverlauf anzeigen.

Aktivieren Sie für jede Zeile, die zu den Diagrammen hinzugefügt werden soll, das Kontrollkästchen. Für jede ausgewählte Zeile wird das Volumen in den Charts für eingehende oder ausgehende Sendungen als Linie angezeigt.



Um sich auf das Verkehrsvolumen für die ausgewählten Einträge zu konzentrieren, können Sie das Gesamtvolumen ausblenden. Um das Gesamtverkehrsvolumen ein- oder auszublenden, aktivieren Sie die Option Gesamtverkehr.



Anzeige des VPC-Datendurchflussverkehrs für EKS-Cluster

Detective hat Einblick in Ihre Amazon Virtual Private Cloud (Amazon VPC)-Datendurchflussprotokolle, die den Datenverkehr darstellen, der Ihre Amazon Elastic Kubernetes Service (Amazon EKS)-Cluster durchquert. Bei Kubernetes-Ressourcen hängt der Inhalt der VPC-Datendurchflussprotokolle vom Container Network Interface (CNI) ab, das im EKS-Cluster bereitgestellt wird.

Ein EKS-Cluster mit einer Standardkonfiguration verwendet das Amazon-VPC-CNI-Plugin. Weitere Informationen finden Sie unter [Verwalten der VPC CNI](#) im Amazon-EKS-Benutzerhandbuch. Das Amazon-VPC-CNI-Plugin sendet internen Datenverkehr mit der IP-Adresse des Pods und übersetzt die Quell-IP-Adresse in die IP-Adresse des Knotens für die externe Kommunikation. Detective kann internen Datenverkehr erfassen und mit dem richtigen Pod korrelieren, dies gilt aber nicht für externen Verkehr.

Wenn Sie möchten, dass Detective Einblick in den externen Datenverkehr Ihrer Pods hat, aktivieren Sie External Source Network Address Translation (SNAT). Die Aktivierung von SNAT ist mit Einschränkungen und Nachteilen verbunden. Weitere Informationen finden Sie unter [SNAT für Pods](#) im Amazon-EKS-Benutzerhandbuch.

Wenn Sie ein anderes CNI-Plugin verwenden, ist Detective nur eingeschränkt auf Pods mit `hostNetwork: true` sichtbar. Für diese Pods zeigt das VPC-Datendurchfluss-Bedienfeld den gesamten Datenverkehr zur IP-Adresse des Pods an. Dies beinhaltet den Datenverkehr zum Hostknoten und zu allen Pods auf dem Knoten mit der Konfiguration `hostNetwork: true`.

Detective zeigt den Verkehr im VPC-Datendurchfluss-Bereich eines EKS-Pods für die folgenden EKS-Cluster-Konfigurationen an:

- In einem Cluster mit dem Amazon-VPC-CNI-Plugin sendet jeder Pod mit der Konfiguration `hostNetwork: false` Datenverkehr innerhalb des Cluster-VPCs.
- In einem Cluster mit dem Amazon VPC CNI-Plugin und der Konfiguration `AWS_VPC_K8S_CNI_EXTERNALSNAT=true` sendet jeder Pod, der Datenverkehr außerhalb der VPC des Clusters `hostNetwork: false` sendet.
- Jeder Pod mit der Konfiguration `hostNetwork: true`. Der Datenverkehr vom Knoten wird mit dem Verkehr von anderen Pods gemischt mit der Konfiguration `hostNetwork: true` vermischt.

Detective zeigt keinen Verkehr im VPC-Datendurchfluss-Bereich an für:

- In einem Cluster mit dem Amazon VPC CNI-Plugin und der Konfiguration `AWS_VPC_K8S_CNI_EXTERNALSNAT=false` sendet jeder Pod mit der Konfiguration `hostNetwork:false`, der Datenverkehr außerhalb des Cluster-VPC sendet.
- In einem Cluster ohne Amazon-VPC-CNI-Plugin für Kubernetes jeder Pod mit der Konfiguration `hostNetwork:false`.
- Jeder Pod, der Traffic an einen anderen Pod sendet, der auf demselben Knoten gehostet wird.

Anzeige des VPC-Datenverkehrs für gemeinsam genutzte Amazon VPCs

Detective hat Einblick in die Flow Logs Ihrer Amazon Virtual Private Cloud (Amazon VPC) für gemeinsam genutzte VPCs:

- Wenn ein Detective-Mitgliedskonto über eine gemeinsam genutzte Amazon VPC verfügt und es andere Nicht-Detective-Konten gibt, die die gemeinsam genutzte VPC verwenden, überwacht Detective den gesamten Datenverkehr von dieser VPC und bietet einen Überblick über den gesamten Datenverkehr in der VPC.
- Wenn Sie eine Amazon-EC2-Instance in einer gemeinsam genutzten Amazon VPC haben und der Eigentümer der gemeinsam genutzten VPC kein Detective-Mitglied ist, überwacht Detective den Datenverkehr von der VPC nicht. Wenn Sie den Datenverkehr innerhalb der VPC anzeigen möchten, müssen Sie den Eigentümer der Amazon VPC als Mitglied Ihres Detective-Diagramms hinzufügen.

Allgemeine Kubernetes-API-Aktivität mit Beteiligung des EKS-Clusters

Die Aktivitätsdetails für die Gesamte Kubernetes-API-Aktivität mit dem EKS-Cluster zeigen die Anzahl der erfolgreichen und fehlgeschlagenen Kubernetes-API-Aufrufe an, die in einem ausgewählten Zeitraum ausgegeben wurden.

Um die Aktivitätsdetails für ein einzelnes Zeitintervall anzuzeigen, wählen Sie das Zeitintervall im Diagramm aus.

Um die Aktivitätsdetails für den aktuellen Zeitbereich anzuzeigen, wählen Sie Details für den Zeitbereich anzeigen aus.

Inhalt der Aktivitätsdetails (Cluster, Pod, Benutzer, Rolle, Rollensitzung)

Für Cluster, Pods, Benutzer, Rollen oder Rollensitzungen enthalten die Aktivitätsdetails die folgenden Informationen:

- Jede Registerkarte enthält Informationen zu den API-Aufrufen, die während des ausgewählten Zeitraums ausgegeben wurden.

Bei Clustern erfolgten die API-Aufrufe innerhalb des Clusters.

Bei Pods zielten die API-Aufrufe auf den Pod ab.

Für Benutzer, Rollen und Rollensitzungen wurden die API-Aufrufe von Kubernetes-Benutzern ausgegeben, die sich als dieser Benutzer, diese Rolle oder diese Rollensitzung authentifiziert hatten.

- Für jeden Eintrag zeigen die Aktivitätsdetails die Anzahl der erfolgreichen, fehlgeschlagenen, nicht autorisierten und verbotenen Aufrufe.
- Zu den Informationen gehören die IP-Adresse, die Art des Kubernetes-Aufrufs, die Entität, die von dem Aufruf betroffen war, und der Betreff (Dienstkonto oder Benutzer), der den Aufruf getätigt hat. Von den Aktivitätsdetails aus können Sie zu den Profilen für die IP-Adresse, den Betreff und die betroffene Entität wechseln.

Die Aktivitätsdetails enthalten die folgenden Tabs:

Betreff

Zeigt zunächst die Liste der Dienstkonten und Benutzer an, die für API-Aufrufe verwendet wurden.

Sie können jedes Dienstkonto und jeden Benutzer erweitern, um die Liste der IP-Adressen anzuzeigen, von denen das Konto oder der Benutzer API-Aufrufe getätigt hat.

Sie können dann jede IP-Adresse erweitern, um die Kubernetes-API-Aufrufe anzuzeigen, die von diesem Konto oder Benutzer von dieser IP-Adresse aus getätigt wurden.

Erweitern Sie den Kubernetes-API-Aufruf, um den `requestURI` zur Identifizierung der ausgeführten Aktion anzuzeigen.

Showing activity: 05/09/2022, 23:00 UTC - 05/10/2022, 23:00 UTC [Edit](#)

Subject | IP address | Kubernetes API call

Filter by Kubernetes subject, IP CIDR, API verb, or API method name

Subject	Success	Failure	Unauthorized	Forbidden
<ul style="list-style-type: none"> cloud-controller-manager Kubernetes user <ul style="list-style-type: none"> 10.0.100.200 IP address <ul style="list-style-type: none"> update 80,343 get 80,343 watch 720 10.0.100.55 IP address 25,245 	186,651	1	0	0

IP-Adresse

Zeigt zunächst die Liste der IP-Adressen an, von denen aus die API-Aufrufe getätigt wurden.

Sie können jeden Aufruf erweitern, um die Liste der Kubernetes-Themen (Dienstkonten und Benutzer) anzuzeigen, die den Aufruf getätigt haben.

Sie können dann jeden Betreff um eine Liste von API-Aufruftypen erweitern, die der Betreff während des Gültigkeitszeitraums getätigt hat.

Erweitern Sie den API-Aufruftyp, um den Aufrug-URI zu sehen, mit dem die ausgeführte Aktion identifiziert werden kann.

Showing activity: 05/09/2022, 23:00 UTC - 05/10/2022, 23:00 UTC [Edit](#)

Subject | **IP address** | Kubernetes API call

Filter by Kubernetes subject, IP CIDR, API verb, or API method name

IP address	Success	Failure	Unauthorized	Forbidden	Location
<ul style="list-style-type: none"> 10.0.100.200 IP address <ul style="list-style-type: none"> cloud-controller-manager Kubernetes user <ul style="list-style-type: none"> update <ul style="list-style-type: none"> /apis/coordination.k8s.io/v1/namespaces/kube-system/leases/cloud-provider-extraction-migration 40,172 /apis/coordination.k8s.io/v1/namespaces/kube-system/leases/cloud-controller-manager 40,171 	599,250	2,706	0	0	-

Kubernetes-API-Aufruf

Zeigt zunächst die Liste der Kubernetes-API-Aufrufverben an.

Sie können jedes API-Verb erweitern, um die mit dieser Aktion verknüpften Aufruf-URIs anzuzeigen.

Sie können dann jeden Aufruf-URI erweitern, um den Kubernetes-Betreff (Dienstkonten und Benutzer) zu sehen, der den API-Aufruf getätigt hat.

Erweitern Sie den Betreff, um zu sehen, welche IPs dieser Betreff für den API-Aufruf verwendet hat.

Resource	Successful calls	Failed calls
Role session	322	310
Role session	91	0
Role session	91	0
config	61	0
kms	15	0
DescribeKey	14	0
ListKeys	1	0
ec2	3	0
secretsmanager	2	0
guardduty	2	0
...

Sortierung der Aktivitätsdetails

Sie können die Aktivitätsdetails nach jeder beliebigen Listenspalte sortieren.

Wenn Sie anhand der ersten Spalte sortieren, wird nur die Liste der obersten Ebene sortiert. Die Listen auf niedrigerer Ebene sind immer nach der Anzahl der erfolgreichen API-Aufrufe sortiert.

Filterung der Aktivitätsdetails

Sie können die Filteroptionen verwenden, um sich auf bestimmte Teilmengen oder Aspekte der Aktivität zu konzentrieren, die in den Aktivitätsdetails dargestellt sind.

Auf allen Registerkarten können Sie die Liste nach beliebigen Werten in der ersten Spalte filtern.

Auswählen des Zeitbereichs für die Aktivitätsdetails

Wenn Sie die Aktivitätsdetails zum ersten Mal anzeigen, entspricht der Zeitraum entweder dem Zeitbereich oder einem ausgewählten Zeitintervall. Sie können den Zeitraum für die Aktivitätsdetails ändern.

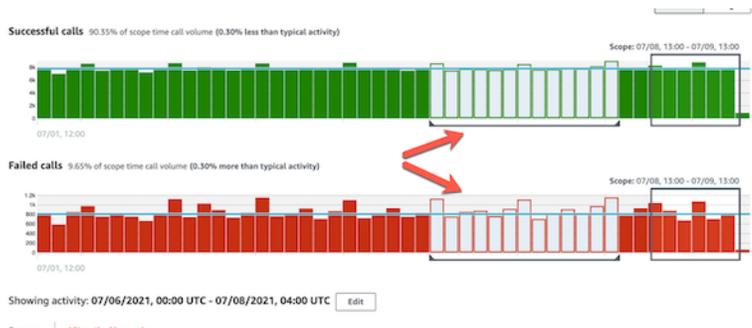
So ändern Sie einen Zeitraum für die Aktivitätsdetails

1. Wählen Sie Bearbeiten aus.
2. Wählen Sie unter Zeitfenster bearbeiten die zu verwendende Start- und Endzeit aus.

Um das Zeitfenster auf die standardmäßige Gültigkeitsdauer für das Profil festzulegen, wählen Sie Auf Standardzeit für den Geltungsbereich festlegen.

3. Wählen Sie Zeitfenster aktualisieren.

Der Zeitraum für die Aktivitätsdetails ist in den Diagrammen des Profilbereichs hervorgehoben.



Verwendung von Anleitungen durch den Profilbereich während einer Untersuchung

Jeder Profilbereich ist darauf ausgelegt, Antworten auf spezifische Fragen zu geben, die sich bei der Durchführung einer Untersuchung und der Analyse der Aktivitäten der betreffenden Entitäten stellen.

Die Anleitungen für jeden Profilbereich helfen Ihnen dabei, diese Antworten zu finden.

Die Anleitung für den Profilbereich beginnt mit einem einzigen Satz im Bereich selbst. Diese Anleitung enthält eine kurze Erläuterung der im Bereich präsentierten Daten.

Um detailliertere Anleitungen für einen Bereich anzuzeigen, wählen Sie in der Bereichsüberschrift Weitere Informationen aus. Diese erweiterte Anleitung wird im Hilfebereich angezeigt.

Die Anleitung kann folgende Arten von Informationen enthalten:

- Einen Überblick über den Inhalt des Bereichs
- Wie benutzt man den Bereich, um die relevanten Fragen zu beantworten
- Vorgeschlagene nächste Schritte auf Grundlage der Antworten

Direkt zu einem Entitätsprofil navigieren oder eine Übersicht finden

Um direkt zu einem Entitätsprofil zu gelangen oder eine Übersicht in Amazon Detective zu finden, können Sie eine dieser Optionen verwenden.

- Von Amazon GuardDuty oder AWS Security Hub aus können Sie von einem GuardDuty Ergebnis zum entsprechenden Findungsprofil von Detective wechseln.
- Sie können eine Detective-URL zusammenstellen, die eine Erkenntnis oder Entität identifiziert und die zu verwendende Gültigkeitsdauer festlegt.

Zu einem Entitätsprofil wechseln oder eine Übersicht von Amazon GuardDuty suchen oder AWS Security Hub

Von der GuardDuty Amazon-Konsole aus können Sie zum Entitätsprofil für eine Entität navigieren, die sich auf einen Befund bezieht.

Von den AWS Security Hub Konsolen GuardDuty und aus können Sie auch zu einer Ergebnisübersicht navigieren. Dort finden Sie auch Links zu den Entitätsprofilen der beteiligten Entitäten.

Diese Links können dazu beitragen, den Untersuchungsprozess zu rationalisieren. Sie können Detective schnell verwenden, um die zugehörige Entitätsaktivität zu sehen und die nächsten Schritte festzulegen. Sie können dann eine Erkenntnis archivieren, falls es sich um eine falsch positive Erkenntnis handelt, oder Sie können das Ausmaß des Problems weiter untersuchen.

So wechseln Sie zur Amazon-Detective-Konsole

Die Links zur Untersuchung sind für alle GuardDuty Ergebnisse verfügbar. GuardDuty ermöglicht es Ihnen auch zu wählen, ob Sie zu einem Entitätsprofil oder zur Ergebnisübersicht navigieren möchten.

Um von der GuardDuty Konsole zu Detective zu wechseln

1. Öffnen Sie die GuardDuty Konsole unter <https://console.aws.amazon.com/guardduty/>.
2. Wählen Sie im linken Navigationsbereich ggf. Erkenntnisse aus.
3. Wählen Sie auf der Seite GuardDuty Ergebnisse das Ergebnis aus.

Der Bereich mit den Erkenntnisdetails wird rechts neben der Erkenntnisliste angezeigt.

4. Wählen Sie im Bereich mit den Erkenntnisdetails die Option In Detective untersuchen.

GuardDuty zeigt eine Liste der verfügbaren Elemente an, die in Detective untersucht werden können.

Die Liste enthält sowohl die zugehörigen Entitäten, wie IP-Adressen oder EC2-Instances, als auch die Erkenntnis.

5. Wählen Sie eine Entität oder Erkenntnis aus.

Die Detective-Konsole wird in einer neuen Registerkarte geöffnet. In der Konsole wird die Entität oder das Erkenntnisprofil geöffnet.

Wenn Sie Detective nicht aktiviert haben, wird auf der Konsole eine Landingpage geöffnet, die einen Überblick über Detective bietet. Von dort aus können Sie wählen, ob Sie Detective aktivieren möchten.

So wechseln Sie von der Security Hub-Konsole zu Detective

1. Öffnen Sie die AWS Security Hub Konsole unter <https://console.aws.amazon.com/securityhub/>.
2. Wählen Sie im linken Navigationsbereich ggf. Erkenntnisse aus.
3. Wählen Sie auf der Seite Security Hub Hub-Ergebnisse ein GuardDuty Ergebnis aus.
4. Wählen Sie im Detailbereich Untersuchung in Detective und dann Untersuchungserkenntnis aus.

Wenn Sie Erkenntnis untersuchen wählen, wird die Detective-Konsole auf einer neuen Registerkarte geöffnet. In der Konsole wird die Übersicht der Erkenntnisse geöffnet.

In der Detective-Konsole wird immer die Region geöffnet, aus der die Erkenntnis stammt, auch wenn Sie aus Ihrer Aggregationsregion wechseln. Weitere Informationen zur Suche nach Aggregation finden Sie im Benutzerhandbuch unter [Aggregieren von Erkenntnissen in verschiedenen Regionen](#).AWS Security Hub

Wenn Sie Detective nicht aktiviert haben, öffnet sich die Konsole mit der Detective-Landingpage. Von dort aus können Sie Detective aktivieren.

Fehlerbehebung für den Pivot

Um den Pivot zu verwenden, muss eine der folgenden Bedingungen erfüllt sein:

- Ihr Konto muss sowohl für Detective als auch für den Dienst, von dem Sie wechseln, ein Administratorkonto sein.
- Sie haben eine kontoübergreifende Rolle übernommen, die Ihrem Administratorkonto Zugriff auf das Verhaltensdiagramm gewährt.

Weitere Informationen zur Empfehlung, Administratorkonten aufeinander abzustimmen, finden Sie unter [Empfohlene Abstimmung mit Amazon GuardDuty und AWS Security Hub](#).

Wenn der Pivot nicht funktioniert, überprüfen Sie Folgendes.

- Gehört die Erkenntnis zu einem aktivierten Mitgliedskonto in Ihrem Verhaltensdiagramm? Wenn das zugehörige Konto nicht als Mitgliedskonto in das Verhaltensdiagramm eingeladen wurde, enthält das Verhaltensdiagramm keine Daten für dieses Konto.

Wenn ein Konto eines eingeladenen Mitglieds die Einladung nicht angenommen hat, enthält das Verhaltensdiagramm keine Daten für dieses Konto.

- Ist die Erkenntnis archiviert? Detective erhält keine archivierten Ergebnisse von GuardDuty.
- Ist die Erkenntnis eingetreten, bevor Detective begann, Daten in Ihr Verhaltensdiagramm aufzunehmen? Wenn die Erkenntnis nicht in den Daten enthalten ist, die Detective aufnimmt, enthält das Verhaltensdiagramm keine Daten dafür.
- Stammt die Erkenntnis aus der richtigen Region? Jedes Verhaltensdiagramm ist spezifisch für eine Region. Ein Verhaltensdiagramm enthält keine Daten aus anderen Regionen.

Navigation zu einem Entitätsprofil oder Übersichtssuche mithilfe einer URL

Um zu einem Entitätsprofil oder einer Suchübersicht in Amazon Detective zu navigieren, können Sie eine URL verwenden, die einen direkten Link dazu enthält. Die URL identifiziert den Befund oder die Entität. Sie kann auch den Zeitbereich angeben, der für das Profil verwendet werden soll. Detective verwaltet historische Ereignisdaten für bis zu einem Jahr.

Format einer Profil-URL

Note

Wenn Sie das alte URL-Format verwenden, leitet Detective automatisch zur neuen URL weiter. Das alte Format der URL war:

```
https://console.aws.amazon.com/detective/home?  
region=Region#type/namespace/instanceID?parameters
```

Das neue Format der Profil-URL lautet wie folgt:

- Für Entitäten – `https://console.aws.amazon.com/detective/home?region=Region#entities/namespace/instanceID?parameters`
- Für Erkenntnisse – `https://console.aws.amazon.com/detective/home?region=Region#findings/instanceID?parameters`

Die URL erfordert die folgenden Werte.

Region

Die Region, die Sie verwenden möchten.

Typ

Der Elementtyp für das Profil, zu dem Sie navigieren.

- `entities` – Zeigt an, dass Sie zu einem Entitätsprofil navigieren
- `findings` – Zeigt an, dass Sie zu einer Erkenntnisübersicht navigieren

Namespace

Bei Entitäten ist der Namespace der Name des Entitätstyps.

- `AwsAccount`
- `AwsRole`
- `AwsRoleSession`
- `AwsUser`
- `Ec2Instance`
- `FederatedUser`
- `IpAddress`
- `S3Bucket`
- `UserAgent`
- `FindingGroup`

- KubernetesSubject
- ContainerPod
- ContainerCluster
- ContainerImage

instanceID

Die Instanz-ID des Befundes oder der Entität.

- Bei einem GuardDuty Befund die Kennung des GuardDuty Befundes.
- Für ein AWS Konto die Konto-ID.
- Für AWS Rollen und Benutzer die Prinzipal-ID der Rolle oder des Benutzers.
- Für Verbundbenutzer die Prinzipal-ID des Verbundbenutzers. Die Prinzipal-ID ist entweder *<identityProvider>:<username>* oder *<identityProvider>:<audience>:<username>*.
- Bei IP-Adressen die IP-Adresse.
- Für Benutzeragenten der Name des Benutzeragenten.
- Für EC2-Instances die Instance-ID.
- Für Rollensitzungen die Sitzungs-ID. Die Sitzungs-ID verwendet das Format *<rolePrincipalID>:<sessionName>*.
- Für S3-Buckets der Bucket-Name.
- Für FindingGroups eine UUID. Zum Beispiel ca6104bc-a315-4b15-bf88-1c1e60998f83
- Verwenden Sie für EKS-Ressourcen die folgenden Formate:
 - EKS-Cluster: *<clusterName>~<accountId>~EKS*
 - *<clusterName><accountId>*Kubernetes-Pod: *~ ~ ~EKS <podUid>*
 - *Kubernetes Betreff: <subjectName>~<clusterName>~<accountId>*
 - Container-Image: *<registry>/<repository>:<tag>@<digest>*

Die Erkenntnis oder die Entität muss mit einem aktivierten Konto in Ihrem Verhaltensdiagramm verknüpft sein.

Die URL kann auch die folgenden optionalen Parameter enthalten, mit denen die Gültigkeitsdauer festgelegt wird. Weitere Informationen zur Gültigkeitsdauer und zu ihrer Verwendung in Profilen finden Sie unter [the section called “Verwaltung des Zeitbereichs”](#).

scopeStart

Startzeit des Zeitbereichs des Profils. Die Startzeit muss innerhalb der letzten 365 Tage liegen.

Der Wert ist der Zeitstempel der Epoche.

Wenn Sie eine Startzeit, aber keine Endzeit angeben, endet die Gültigkeitsdauer zum aktuellen Zeitpunkt.

scopeEnd

Endzeit des Zeitbereichs des Profils.

Der Wert ist der Zeitstempel der Epoche.

Wenn Sie eine Endzeit, aber keine Startzeit angeben, umfasst der Zeitbereich die gesamte Zeit vor der Endzeit.

Wenn Sie den Zeitbereich nicht angeben, wird der Standardzeitbereich verwendet.

- Für Erkenntnisse verwendet der Standard-Zeitbereich den Zeitpunkt, zu dem die Erkenntnisaktivität zum ersten und zum letzten Mal beobachtet wurde.
- Für Entitäten entspricht der Standard-Zeitbereich den letzten 24 Stunden.

Hier finden Sie ein Beispiel für eine Detective-URL:

```
https://console.aws.amazon.com/detective/home?region=us-east-1#entities/  
IpAddress/192.168.1.1?scopeStart=1552867200&scopeEnd=1552910400
```

Diese Beispiel-URL enthält die folgenden Anweisungen.

- Zeigen Sie das Entitätsprofil für die IP-Adresse 192.168.1 an.
- Verwenden Sie eine Gültigkeitsdauer, die am Montag, den 18. März 2019, 12:00:00 Uhr GMT beginnt und am Montag, den 18. März 2019, 12:00:00 Uhr GMT endet.

Fehlerbehebung bei einer URL

Wenn die URL nicht das erwartete Profil anzeigt, überprüfen Sie zunächst, ob die URL das richtige Format verwendet und ob Sie die richtigen Werte angegeben haben.

- Haben Sie mit der richtigen URL (*findings* oder *entities*) angefangen?

- Haben Sie den richtigen Namespace angegeben?
- Haben Sie den richtigen Bezeichner angegeben?

Wenn die Werte korrekt sind, können Sie auch Folgendes überprüfen.

- Gehört die Erkenntnis oder die Entität zu einem aktivierten Mitgliedskonto in Ihrem Verhaltensdiagramm? Wenn das zugehörige Konto nicht als Mitgliedskonto in das Verhaltensdiagramm eingeladen wurde, enthält das Verhaltensdiagramm keine Daten für dieses Konto.

Wenn ein Konto eines eingeladenen Mitglieds die Einladung nicht angenommen hat, enthält das Verhaltensdiagramm keine Daten für dieses Konto.

- Ist eine Erkenntnis archiviert? Detective erhält keine archivierten Ergebnisse von Amazon GuardDuty.
- Ist die Erkenntnis oder Entität eingetreten, bevor Detective begann, Daten in Ihr Verhaltensdiagramm aufzunehmen? Wenn die Erkenntnis oder die Entität nicht in den Daten enthalten ist, die Detective aufnimmt, enthält das Verhaltensdiagramm keine Daten dafür.
- Stammt die Erkenntnis oder Entität aus der richtigen Region? Jedes Verhaltensdiagramm ist spezifisch für eine Region. Ein Verhaltensdiagramm enthält keine Daten aus anderen Regionen.

Hinzufügen von Detective-URLs für Erkenntnisse zu Splunk

Das Splunk Trumpet-Projekt ermöglicht es Ihnen, Daten von Diensten an Splunk zu senden. AWS

Sie können das Trumpet-Projekt so konfigurieren, dass Detektiv-URLs für GuardDuty Amazon-Ergebnisse generiert werden. Sie können diese URLs dann verwenden, um direkt von Splunk zu den entsprechenden Erkenntnisprofilen von Detective zu wechseln.

[Das Trumpet-Projekt ist GitHub unter https://github.com/splunk/splunk-aws-project-trumpet verfügbar.](https://github.com/splunk/splunk-aws-project-trumpet)

Wählen Sie auf der Konfigurationsseite für das Trumpet-Projekt unter AWS CloudWatch Ereignisse die Option Detective GuardDuty URLs aus.

Verwaltung des Zeitbereichs

Passen Sie den Zeitbereich an, der zur Begrenzung der in Entitätsprofilen angezeigten Daten verwendet wird.

Die Diagramme, Zeitpläne und anderen Daten, die in Entitätsprofilen angezeigt werden, basieren alle auf dem aktuellen Zeitbereich. Der Zeitbereich ist die Übersicht der Aktivitäten einer Entität im Zeitverlauf. Dies wird oben rechts in jedem Profil in der Amazon-Detective-Konsole angezeigt. Die in diesen Diagrammen, Zeitplänen und anderen Visualisierungen angezeigten Daten basieren auf der Gültigkeitsdauer. Bei einigen Profilbereichen wird zusätzliche Zeit vor und nach dem Zeitbereich hinzugefügt, um den Kontext bereitzustellen. In Detective werden alle Zeitstempel standardmäßig in UTC angezeigt. Sie können Ihre lokale Zeitzone auswählen, indem Sie die Zeitstempel-Einstellungen ändern. Informationen zum Aktualisieren der Zeitstempel-Einstellung finden Sie unter [the section called “Festlegen des Zeitstempelformats”](#).

Detective Analytics verwendet den Zeitbereich, um nach ungewöhnlichen Aktivitäten zu suchen. Der Analyseprozess erfasst die Aktivität während des Zeitbereichs und vergleicht sie dann mit der Aktivität in den 45 Tagen vor dem Zeitbereich. Außerdem wird dieser Zeitraum von 45 Tagen verwendet, um Basiswerte für Aktivitäten zu generieren.

In einer Übersicht über die Erkenntnisse gibt die Dauer des Umfangs an, wann die Erkenntnis zum ersten und zum letzten Mal beobachtet wurde. Weitere Informationen zur Erkenntnisübersicht finden Sie unter [the section called “Überblick über Erkenntnisse”](#).

Während Sie eine Untersuchung durchführen, können Sie den Zeitbereich anpassen. Wenn die ursprüngliche Analyse beispielsweise auf Aktivitäten an einem einzigen Tag beruhte, möchten Sie diese möglicherweise auf eine Woche oder einen Monat ausweiten. Der erweiterte Zeitraum könnte Ihnen helfen, ein besseres Gefühl dafür zu bekommen, ob die Aktivität einem normalen Muster entspricht oder ungewöhnlich ist.

Sie können den Zeitbereich auch so festlegen, dass er einer zugehörigen Erkenntnis für die aktuelle Entität entspricht.

Wenn Sie den Zeitbereich ändern, wiederholt Detective seine Analyse und aktualisiert die angezeigten Daten auf Grundlage des neuen Zeitbereichs.

Der Zeitbereich darf nicht kürzer als eine Stunde und nicht länger als ein Jahr sein. Die Start- und Endzeit müssen auf einer Stunde liegen.

Festlegen des spezifischen Start- und Enddatums und der Uhrzeiten

Sie können das Start- und Enddatum des Zeitbereichs in der Detective-Konsole festlegen.

So legen Sie bestimmte Start- und Endzeiten für den neuen Zeitbereich fest

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.

2. Wählen Sie in einem Entitätsprofil den Zeitbereich aus.
3. Wählen Sie im Bereich Zeitbereich bearbeiten unter Start das neue Startdatum und die neue Startzeit für den Zeitbereich aus. Für die neue Startzeit wählen Sie nur die Stunde aus.
4. Wählen Sie unter Ende das neue Enddatum und die neue Endzeit für den Zeitbereich aus. Für die neue Endzeit wählen Sie nur die Stunde aus. Die Endzeit muss mindestens eine Stunde nach der Startzeit liegen.
5. Wenn Sie mit der Bearbeitung fertig sind, wählen Sie Zeitbereich aktualisieren, um die Änderungen zu speichern und die angezeigten Daten zu aktualisieren.

Bearbeiten der Zeitdauer für den Zeitbereich

Wenn Sie eine Zeitdauer für den Zeitbereich festlegen, legt Detective den Zeitbereich auf diese Zeitspanne ab der aktuellen Uhrzeit fest.

So bearbeiten Sie die Zeitdauer für den Zeitbereich

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie in einem Entitätsprofil den Zeitbereich aus.
3. Wählen Sie im Bereich Zeitbereich bearbeiten neben Historisch den Zeitraum für den Zeitbereich aus.

Wenn Sie einen Zeitraum angeben, werden die Start - und Endeinstellungen aktualisiert.

4. Wenn Sie mit der Bearbeitung fertig sind, wählen Sie Zeitbereich aktualisieren, um die Änderungen zu speichern und die angezeigten Daten zu aktualisieren.

Stellen Sie den Zeitbereich auf ein Zeitfenster für die Suche ein

Jede Erkenntnis ist ein Zeitfenster zugeordnet, das angibt, wann die Erkenntnis zum ersten und zum letzten Mal beobachtet wurde. Wenn Sie sich eine Erkenntnisübersicht ansehen, ändert sich der Zeitbereich zum Zeitfenster für die Erkenntnisse.

In einem Entitätsprofil können Sie den Zeitbereich an das Zeitfenster für eine zugeordnete Erkenntnis anpassen. Auf diese Weise können Sie die Aktivität untersuchen, die in diesem Zeitraum stattgefunden hat.

Wählen Sie im Bereich Zugeordnete Erkenntnisse die Erkenntnis aus, die Sie verwenden möchten, um den Zeitbereich an ein Zeitfenster für die Erkenntnisse anzupassen.

Detective füllt die Erkenntnisdetails aus und legt die Gültigkeitsdauer auf das Suchzeitfenster fest.

Festlegen des Zeitbereichs auf der Übersichtsseite

Wenn Sie sich die Übersichtsseite ansehen, können Sie den Zeitbereich für den Umfang anpassen, sodass Sie sich die Aktivität für einen beliebigen 24-Stunden-Zeitraum der letzten 365 Tage ansehen können.

So legen Sie den Zeitbereich auf der Übersichtsseite fest

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Detective-Navigationsbereich Übersicht aus.
3. Im Bereich Zeitbereich können Sie neben Übersicht das Startdatum und die Startzeit ändern. Die Startzeit muss innerhalb der letzten 365 Tage liegen.

Wenn Sie das Startdatum und die Startzeit ändern, werden das Enddatum und die Endzeit automatisch auf 24 Stunden nach der ausgewählten Startzeit aktualisiert.

Note

Mit Detective können Sie auf historische Ereignisdaten von bis zu einem Jahr zugreifen. Weitere Informationen zu Quelldaten in Detective finden Sie unter [In einem Verhaltensdiagramm verwendete Quelldaten](#).

4. Wenn Sie mit der Bearbeitung fertig sind, wählen Sie Zeitbereich aktualisieren, um die Änderungen zu speichern und die angezeigten Daten zu aktualisieren.

Details zu den zugehörigen Erkenntnissen ansehen

Jedes Entitätsprofil enthält einen zugehörigen Erkenntnisbereich, in dem die Erkenntnis aufgeführt sind, an denen die Entität im aktuellen Zeitbereich beteiligt war. Ein Anzeichen dafür, dass eine Entität kompromittiert wurde, ist ihre Beteiligung an mehreren Erkenntnissen. Die Art der Erkenntnisse kann auch Aufschluss über die Art der Aktivität geben, über die man sich Sorgen machen muss.

Der zugehörige Erkenntnisbereich wird unmittelbar unter dem Profilbereich mit den Entitätsdetails angezeigt.

Für jede Erkenntnis umfasst die Tabelle Informationen über Folgendes:

- Der Titel der Erkenntnisse, der auch ein Link zur Erkenntnisübersicht ist.
- Das mit dem Befund verknüpfte AWS Konto, das auch ein Link zum Kontoprofil ist
- Den Erkenntnistyp
- Der früheste Zeitpunkt, zu dem der Befund beobachtet wurde
- Der Zeitpunkt, zu dem der Befund zuletzt beobachtet wurde
- Den Schweregrad einer Erkenntnis

Um die Erkenntnisdetails für eine Erkenntnis anzuzeigen, wählen Sie das Optionsfeld für die Erkenntnis. Detective füllt den Bereich mit den Erkenntnisdetails rechts auf der Seite aus. Detective ändert auch den Zeitbereich in das Erkenntnis-Zeitfenster. So können Sie sich auf Aktivitäten konzentrieren, die in diesem Zeitraum stattgefunden haben.

Wenn Sie von einer Erkenntnisübersicht zum Entitätsprofil navigiert sind, wird diese Erkenntnis automatisch ausgewählt und die Details für die Erkenntnis werden angezeigt.

Wählen Sie in den Erkenntnisdetails die Option Alle verwandten Entitäten anzeigen aus, um zurück zur Erkenntnisübersicht zu gelangen.

Sie können die Erkenntnis auch archivieren. Siehe [the section called “Archivierung eines GuardDuty Befundes”](#).

Details für Entitäten mit hohem Volumen anzeigen

Im [Verhaltensdiagramm](#) verfolgt Amazon Detective Beziehungen zwischen Entitäten. In jedem Verhaltensdiagramm wird beispielsweise nachverfolgt, wann ein AWS Benutzer eine AWS Rolle erstellt und wann eine EC2-Instance eine Verbindung zu einer IP-Adresse herstellt.

Wenn eine Entität in einem bestimmten Zeitraum zu viele Beziehungen hat, kann Detective nicht alle Beziehungen speichern. Wenn dies während der aktuellen Gültigkeitsdauer der Fall ist, werden Sie von Detective benachrichtigt. Detective bietet auch eine Liste der Vorkommen von Entitäten mit hohem Volumen.

Was ist eine Entität mit hohem Volumen?

Während eines bestimmten Zeitintervalls kann eine Entität der Ursprung oder das Ziel einer extrem großen Anzahl von Verbindungen sein. Beispielsweise kann eine EC2-Instance Verbindungen von Millionen von IP-Adressen haben.

Detective begrenzt die Anzahl der Verbindungen, die es in jedem Zeitintervall aufnehmen kann. Wenn eine Entität dieses Limit überschreitet, verwirft Detective die Verbindungen für dieses Zeitintervall.

Nehmen wir zum Beispiel an, dass das Limit bei 100.000.000 Verbindungen pro Zeitintervall liegt. Wenn eine EC2-Instance während eines Zeitintervalls über mehr als 100.000.000 IP-Adressen verbunden ist, verwirft Detective die Verbindungen aus diesem Zeitintervall.

Möglicherweise können Sie diese Aktivität jedoch anhand der Entität am anderen Ende der Beziehung analysieren. Um das Beispiel fortzusetzen: Eine EC2-Instance kann zwar von Millionen von IP-Adressen aus verbunden werden, eine einzelne IP-Adresse stellt jedoch eine Verbindung zu weit weniger EC2-Instances her. Jedes IP-Adressprofil enthält Details zu den EC2-Instances, mit denen die IP-Adresse verbunden ist.

Anzeige der Benachrichtigung über Entitäten mit hohem Volumen in einem Profil

Detective zeigt oben in einem Befund- oder Entitätsprofil einen Hinweis an, wenn die Gültigkeitsdauer ein Zeitintervall umfasst, in dem die Entität ein hohes Volumen aufweist. Bei der Suche nach Profilen bezieht sich der Hinweis auf die betroffene Entität.

Die Mitteilung enthält eine Liste der Beziehungen, die umfangreiche Zeitintervalle aufweisen. Jeder Listeneintrag enthält eine Beschreibung der Beziehung und den Beginn des Zeitintervalls mit hohem Datenvolumen.

Ein Zeitintervall mit hohem Volumen kann ein Indikator für verdächtige Aktivitäten sein. Um zu verstehen, welche anderen Aktivitäten gleichzeitig stattfanden, können Sie Ihre Untersuchung auf ein Zeitintervall mit hohem Datenvolumen konzentrieren. Die Mitteilung von Unternehmen mit hohem Volumen enthält eine Option, mit der Sie den Umfang auf dieses Zeitintervall festlegen können.

So legen Sie die Gültigkeitsdauer auf ein Zeitintervall mit hohem Volumen fest

1. Wählen Sie in der großvolumigen Entitätsmitteilung das Zeitintervall aus.
2. Wählen Sie im Popupmenü die Option Geltungsdauer anwenden aus.

Die Liste der Entitäten mit hohem Volumen für den aktuellen Gültigkeitszeitraum anzeigen

Die Seite Entitäten mit hohem Volumen enthält eine Liste der Zeitintervalle und Entitäten mit hohem Volumen während des aktuellen Gültigkeitszeitraums.

So zeigen Sie die Seite mit Entitäten mit hohem Volumen an

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich von Detective die Option Entitäten mit hohem Volumen aus.

Jedes Listenelement enthält die folgenden Informationen.

- Beginn des Zeitintervalls mit hohem Volumen
- Die ID und die Art der Entität
- Die Beschreibung der Beziehung, z. B. „Die EC2-Instance wurde über eine IP-Adresse verbunden“

Sie können die Liste nach einer beliebigen Spalte filtern und sortieren. Sie können auch zum Entitätsprofil einer beteiligten Entität navigieren.

So navigieren Sie zum Profil für eine Entität

1. Wählen Sie in der Liste der Entitäten mit hohem Volumen die Zeile aus, aus der Sie navigieren möchten.
2. Wählen Sie Profil mit umfangreichem Umfang anzeigen aus.

Wenn Sie diese Option verwenden, um zu einem Entitätsprofil zu navigieren, wird die Gültigkeitsdauer wie folgt festgelegt:

- Die Geltungsdauer beginnt 30 Tage vor dem Zeitintervall für hohe Datenvolumen.
- Die Gültigkeitsdauer endet am Ende des Zeitintervalls für hohe Datenvolumen.

Verwaltung von Ergebnissen und Entitäten

Amazon Detective bietet mehrere wichtige Funktionen, mit denen Sie Ihre Ergebnisse suchen, exportieren und verwalten können. Diese Funktionen helfen Ihnen dabei, die Ergebnisse an Ihre spezifische Umgebung anzupassen, das Rauschen aufgrund von Ergebnissen mit geringem Wert zu reduzieren und sich auf Bedrohungen für Ihre individuelle AWS Umgebung zu konzentrieren. Lesen Sie die Themen auf dieser Seite, um zu erfahren, wie Sie diese Funktionen nutzen können, um den Wert der Ergebnisse von Detective zu steigern.

Inhalt

- [Suche nach einer Erkenntnis oder Entität](#)
- [Exportieren von Daten aus Detective](#)
- [Archivierung eines GuardDuty Amazon-Befundes](#)

Suche nach einer Erkenntnis oder Entität

Mit der Suchfunktion von Amazon Detective können Sie nach einer Erkenntnis oder Entität suchen. Von den Suchergebnissen aus können Sie zu einem Entitätsprofil oder einer Erkenntnisübersicht navigieren. Wenn Ihre Suche mehr als 10.000 Erkenntnisse zurückgibt, werden nur die 10.000 besten Erkenntnisse angezeigt. Wenn Sie die Sortierreihenfolge ändern, werden auch die zurückgegebenen Erkenntnisse geändert.

Sie können Ihre Suchergebnisse in eine .csv-Datei (komma-getrennte Werte) exportieren. Diese Datei enthält die auf der Suchseite zurückgegebenen Daten. Weitere Informationen finden Sie unter [the section called “Exportieren von Daten aus Detective”](#).

Abschließen der Suche

Um die Suche abzuschließen, wählen Sie den Typ der Entität aus, nach der gesucht werden soll. Geben Sie dann den genauen Bezeichner oder den Bezeichner mit Platzhalterzeichen * oder ? ein. Um nach einer Reihe von IP-Adressen zu suchen, können Sie auch CIDR oder Punktnotationen verwenden. Sehen Sie sich die folgenden Beispiel-Suchzeichenfolgen an.

Für IP-Adressen:

- 1.0.*.*

- 1.0.133.*
- 1.0.0.0/16
- 0.239.48.198/31

Für alle anderen Arten von Entitäten:

- Admin
- ad*
- ad*n
- ad*n*
- adm?n
- a?m*
- *min

Für jeden Entitätstyp werden die folgenden Bezeichner unterstützt:

- Für Erkenntnisse, die Erkenntnis-ID oder den Amazon-Ressourcennamen (ARN) der Erkenntnis.
- Für AWS Konten die Konto-ID.
- Für AWS Rollen und AWS Benutzer entweder die Prinzipal-ID, der Name oder der ARN.
- Für Container-Cluster der Clustername oder ARN.
- Für Container-Images das Repository oder der vollständige Digest des Container-Images.
- Für Container-Pods oder Tasks der Pod-Name oder die UID des Pods.
- Für EC2-Instances die Instance-ID oder der ARN.
- Für die Erkenntnisgruppe die ID der Erkenntnisgruppe.
- Die IP-Adressen, die Adresse in CIDR oder die Dot-Notation.
- Für Kubernetes-Themen (Dienstkonten oder Benutzer) der Name.
- Für einer Rollensitzung können Sie einen der folgenden Werte für die Suche verwenden:
 - Die Rollensitzungs-ID.

Die Rollensitzungs-ID verwendet das Format *<rolePrincipalID>:<sessionName>*.

Hier ist ein Beispiel: AR0A12345678910111213:MySession.

- Rollensitzungs-ARN

- Sitzungsname
- Prinzipal-ID der Rolle, die übernommen wurde
- Name der Rolle, die übernommen wurde
- Für S3-Buckets der Bucket-Name oder der Bucket-ARN.
- Für Verbundbenutzer die Prinzipal-ID oder der Benutzername. Die Prinzipal-ID ist entweder `<identityProvider>:<username>` oder `<identityProvider>:<audience>:<username>`.
- Für Benutzeragenten der Name des Benutzeragenten.

So suchen Sie nach einem Befund oder einer Entität

1. Melden Sie sich bei der an AWS Management Console. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Klicken Sie im Navigationsbereich auf Suchen.
3. Wählen Sie im Menü Typ auswählen den Elementtyp aus, nach dem Sie suchen.

Beachten Sie, dass Sie bei der Auswahl von Benutzer entweder nach einem AWS -Benutzer oder einem Verbundbenutzer suchen können.

Beispiele aus Ihren Daten enthalten einen Beispielsatz von Identifikatoren des ausgewählten Typs, die in Ihren Verhaltensdiagrammdateien enthalten sind. Um das Profil für eines der Beispiele anzuzeigen, wählen Sie dessen Kennung aus.

4. Geben Sie die genaue Kennung oder eine Kennung mit Platzhalterzeichen ein, nach der gesucht werden soll.

Bei der Suche muss die Groß- und Kleinschreibung nicht beachtet werden.

5. Wählen Sie Suchen, oder drücken Sie die Eingabetaste.

Verwenden der Suchergebnisse

Wenn Sie die Suche abgeschlossen haben, zeigt Detective eine Liste mit bis zu 10.000 passenden Ergebnissen an. Bei Suchanfragen, die eine eindeutige Kennung verwenden, gibt es nur ein passendes Ergebnis.

Wählen Sie aus den Ergebnissen die Kennung aus, um zum Entitätsprofil oder zur Erkenntnisübersicht zu gelangen.

Für Erkenntnisse, Rollen, Benutzer und EC2-Instances enthalten die Suchergebnisse das zugehörige Konto. Um zum Profil für das Konto zu navigieren, wählen Sie die Konto-ID aus.

Fehlerbehebung bei der Suche

Wenn Detective den Befund oder die Entität nicht findet, überprüfen Sie zunächst, ob Sie die richtige Kennung eingegeben haben. Wenn die Kennung korrekt ist, können Sie auch Folgendes überprüfen.

- Gehört die Erkenntnis oder die Entität zu einem aktivierten Mitgliedskonto in Ihrem Verhaltensdiagramm? Wenn das zugehörige Konto nicht als Mitgliedskonto in das Verhaltensdiagramm eingeladen wurde, enthält das Verhaltensdiagramm keine Daten für dieses Konto.

Wenn ein Konto eines eingeladenen Mitglieds die Einladung nicht angenommen hat, enthält das Verhaltensdiagramm keine Daten für dieses Konto.

- Ist eine Erkenntnis archiviert? Detective erhält keine archivierten Ergebnisse von Amazon GuardDuty.
- Ist die Erkenntnis oder Entität eingetreten, bevor Detective begann, Daten in Ihr Verhaltensdiagramm aufzunehmen? Wenn die Erkenntnis oder die Entität nicht in den Daten enthalten ist, die Detective aufnimmt, enthält das Verhaltensdiagramm keine Daten dafür.
- Stammt die Erkenntnis oder Entität aus der richtigen Region? Jedes Verhaltensdiagramm ist spezifisch für einen AWS-Region. Ein Verhaltensdiagramm enthält keine Daten aus anderen Regionen.

Exportieren von Daten aus Detective

Sie können Daten von der Amazon-Detective-Übersichtsseite und der Suchergebnisseite exportieren. Die Daten werden im CSV-Format (komma-getrennte Werte) exportiert. Der Dateiname der exportierten Daten folgt dem Musterformat `detective-page-panel-yyyy-mm-dd.csv`. Sie können Ihre Sicherheitsprüfungen bereichern, indem Sie die Daten mithilfe anderer AWS-Services, Drittanbieteranwendungen oder Tabellenkalkulationsprogramme ändern, die den CSV-Import unterstützen.

Note

Wenn gerade ein Export ausgeführt wird, warten Sie, bis der Export abgeschlossen ist, bevor Sie versuchen, weitere Daten zu exportieren.

Sie können in Detective eine CSV-Datei (komma-getrennte Werte) exportieren, die aus den folgenden Bereichen und Seiten besteht:

- Übersichtsseite
 - Bereich Rollen und Benutzer mit dem höchsten API-Aufrufvolumen
 - Bereich für EC2-Instances mit dem höchsten Traffic-Volumen
 - Bereich für EKS-Cluster mit den meisten erstellten Kubernetes-Pods
- Suchseite – Wenn Ihre Suche mehr als 10.000 Ergebnisse zurückgibt, werden nur die 10.000 besten Ergebnisse exportiert. Wenn Sie die Sortierreihenfolge ändern, werden auch die zurückgegebenen Erkenntnisse geändert.

Archivierung eines GuardDuty Amazon-Befundes

Wenn Sie Ihre Untersuchung eines GuardDuty Amazon-Befundes abgeschlossen haben, können Sie das Ergebnis von Amazon Detective archivieren. Dies erspart Ihnen die Mühe, zur Aktualisierung zurückkehren GuardDuty zu müssen. Die Archivierung einer Erkenntnis bedeutet, dass Sie Ihre Untersuchung abgeschlossen haben.

Sie können einen GuardDuty Befund nur dann in Detective archivieren, wenn Sie auch das GuardDuty Administratorkonto für das Konto sind, das dem Befund zugeordnet ist. Wenn Sie kein GuardDuty Administratorkonto haben und versuchen, einen Befund zu archivieren, GuardDuty wird ein Fehler angezeigt.

Um einen GuardDuty Befund zu archivieren

1. Wählen Sie in der Detective-Konsole im Bereich mit den Erkenntnisdetails die Option Erkenntnis archivieren aus.
2. Wenn Sie aufgefordert werden, Ihre Entscheidung zu bestätigen, wählen Sie Archiv aus.

Sie können archivierte GuardDuty Ergebnisse in der GuardDuty Konsole anzeigen. Weitere Informationen finden Sie unter [Suppression Rules](#) im GuardDuty Amazon-Benutzerhandbuch.

Verwalten von Konten

Jedes Verhaltensdiagramm enthält Daten von einem oder mehreren Konten. Wenn ein Konto Detective aktiviert, wird es zum Administratorkonto für das Verhaltensdiagramm und wählt die Mitgliedskonten für das Verhaltensdiagramm aus. Ein Verhaltensdiagramm kann bis zu 1.200 Mitgliedskonten enthalten.

Wenn Sie integriert sind AWS Organizations, bestimmt das Organisationsverwaltungskonto das Detective-Administratorkonto für die Organisation. Dieses Detective-Administratorkonto wird dann zum Administratorkonto für das Verhaltensdiagramm der Organisation. Das Detective Administrator-Konto kann jedes Organisationskonto als Mitgliedskonto im Verhaltensdiagramm der Organisation aktivieren. Organizations-Konten können sich nicht vom Verhaltensdiagramm der Organisation trennen.

Ein Administratorkonto kann Konten auch dazu einladen, einem Verhaltensdiagramm beizutreten. Wenn das Konto die Einladung annimmt, aktiviert Detective das Konto als Mitgliedskonto. Mitgliedskonten, die auf Einladung hinzugefügt werden, können sich aus dem Verhaltensdiagramm entfernen.

Wenn ein Konto als Mitgliedskonto aktiviert ist, beginnt Detective, die Daten des Mitgliedskontos aufzunehmen und in dieses Verhaltensdiagramm zu extrahieren.

Detective berechnet jedem Konto die Daten, die es zu jedem Verhaltensdiagramm beiträgt. Informationen zur Nachverfolgung des Datenvolumens für jedes Konto in einem Verhaltensdiagramm finden Sie unter [Prognose und Überwachung der Amazon Detective-Kosten](#).

Inhalt

- [Kontobeschränkungen und Empfehlungen in Detective](#)
- [Umstellung auf die Nutzung von Organizations zur Verwaltung von Verhaltensdiagramm-Konten](#)
- [Festlegen des Detective-Administratorkontos für eine Organisation](#)
- [Verfügbare Aktionen für Konten](#)
- [Anzeige der Kontenliste](#)
- [Organisationskonten als Mitgliedskonten verwalten](#)
- [Mitgliedskonten eingeladener Mitglieder verwalten](#)
- [Für Mitgliedskonten: Einladungen und Mitgliedschaften im Verhaltensdiagramm verwalten](#)
- [Auswirkung von Kontoaktionen auf Verhaltensdiagramme](#)

- [Verwenden der Amazon Detective Python-Skripte zur Verwaltung von Konten](#)

Kontobeschränkungen und Empfehlungen in Detective

Seien Sie sich der folgenden Beschränkungen bewusst, wenn Sie Konten in Amazon Detective verwalten.

Maximale Anzahl von Mitgliedern pro Konto

Detective erlaubt bis zu 1.200 Mitgliedskonten in jedem Verhaltensdiagramm.

Konten und Regionen

Wenn Sie Konten verwalten AWS Organizations, bestimmt das Organisationsverwaltungskonto ein Detective-Administratorkonto für die Organisation. Das Detective-Administratorkonto wird zum Administratorkonto für das Verhaltensdiagramm der Organisation.

Das Detective-Administratorkonto muss in allen Regionen identisch sein. Das Verwaltungskonto der Organisation bestimmt das Detective-Administratorkonto in jeder Region separat. Das Detective-Administratorkonto verwaltet auch die Verhaltensdiagramme der Organisation und die Mitgliedskonten in jeder Region separat.

Bei Mitgliedskonten, die auf Einladung erstellt wurden, wird die Zuordnung zwischen Administrator und Mitglied nur in der Region erstellt, aus der die Einladung gesendet wurde. Das Administratorkonto muss Detective in jeder Region aktivieren und verfügt in jeder Region über ein separates Verhaltensdiagramm. Das Administratorkonto lädt dann jedes Konto ein, es als Mitgliedskonto in dieser Region zu verknüpfen.

Ein Konto kann ein Mitgliedskonto mit mehreren Verhaltensdiagrammen in derselben Region sein. Ein Konto kann nur das Administratorkonto für ein Verhaltensdiagramm pro Region sein. Ein Konto kann ein Administratorkonto in verschiedenen Regionen sein.

Abstimmung der Administratorkonten mit Security Hub und GuardDuty

Um sicherzustellen, dass die Integrationen mit AWS Security Hub und Amazon reibungslos GuardDuty funktionieren, empfehlen wir, bei all diesen Diensten dasselbe Konto als Administratorkonto zu verwenden.

Siehe [the section called "Empfohlene Ausrichtung mit und GuardDuty AWS Security Hub"](#).

Gewährung der erforderlichen Berechtigungen für Administratorkonten

Um sicherzustellen, dass ein Administratorkonto über die erforderlichen Berechtigungen zur Verwaltung seines Verhaltensdiagramms verfügt, fügen Sie die [AmazonDetectiveFullAccessVerwaltete Richtlinie](#) dem IAM-Prinzipal hinzu.

Reflektieren von Organisationsaktualisierungen in Detective

Änderungen an einer Organisation spiegeln sich nicht sofort in Detective wider.

Bei den meisten Änderungen, z. B. bei neuen und entfernten Unternehmenskonten, kann es bis zu einer Stunde dauern, bis Detective benachrichtigt wird.

Die Weitergabe einer Änderung am designierten Detective-Administratorkonto in Organizations nimmt weniger Zeit in Anspruch.

Umstellung auf die Nutzung von Organizations zur Verwaltung von Verhaltensdiagramm-Konten

Möglicherweise verfügen Sie über ein vorhandenes Verhaltensdiagramm mit Mitgliedskonten, die eine manuelle Einladung akzeptiert haben. Wenn Sie registriert sind, gehen Sie wie folgt vor AWS Organizations, um mithilfe von Organizations Mitgliedskonten zu aktivieren und zu verwalten, anstatt den manuellen Einladungsprozess zu verwenden:

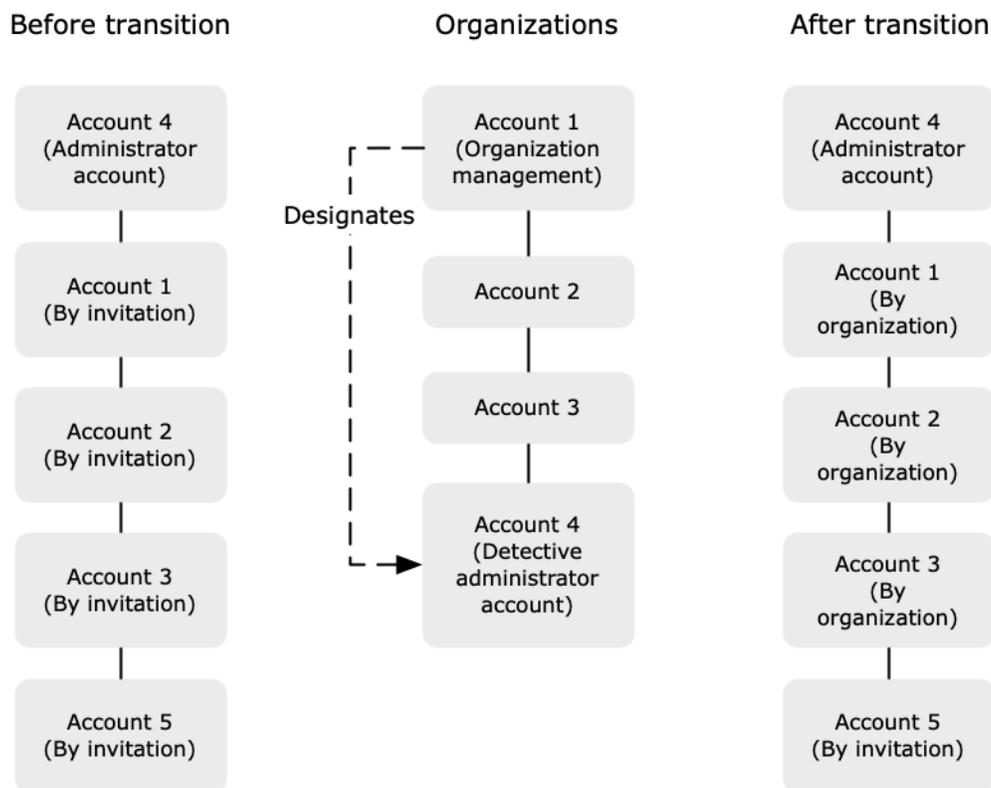
1. [Legen Sie das Detective-Administratorkonto für Ihre Organisation fest.](#) Dadurch wird das Verhaltensdiagramm der Organisation erstellt.

Wenn das Detective-Administratorkonto bereits über ein Verhaltensdiagramm verfügt, wird dieses Verhaltensdiagramm zum Verhaltensdiagramm der Organisation.

2. [Aktivieren Sie Organisationskonten als Mitgliedskonten im Verhaltensdiagramm der Organisation.](#)

Wenn das Verhaltensdiagramm der Organisation bereits Mitgliedskonten enthält, bei denen es sich um Organisationskonten handelt, werden diese Konten automatisch aktiviert.

Das folgende Diagramm zeigt einen Überblick über die Struktur eines Verhaltensdiagramms vor der Umstellung, die Konfiguration in Organizations und die Kontostruktur des Verhaltensdiagramms nach der Umstellung.



Festlegen eines Detective-Administratorkontos für Ihre Organisation

Ihr Verwaltungskonto Ihrer Organisation bestimmt das Detective-Administratorkonto Ihrer Organisation. Siehe [the section called “Festlegen des Detective-Administratorkontos”](#).

Um den Übergang zu vereinfachen, empfiehlt Detective, dass Sie ein aktuelles Administratorkonto als Detective-Administratorkonto für die Organisation wählen.

Wenn es ein delegiertes Administratorkonto für Detective in Organizations gibt, müssen Sie entweder dieses Konto oder das Verwaltungskonto Ihrer Organisation als Detective-Administratorkonto verwenden.

Andernfalls ruft Detective Organizations auf, wenn Sie zum ersten Mal ein Detective-Administratorkonto festlegen, das nicht das Verwaltungskonto Ihrer Organisation ist, um dieses Konto zum delegierten Administratorkonto für Detective zu machen.

Organisationskonten als Mitgliedskonten aktivieren

Das delegierte Administratorkonto für Detective ist das Administratorkonto für das Verhaltensdiagramm des Unternehmens. Das Detective-Administratorkonto wählt die

Organisationskonten aus, die als Mitgliedskonten im Diagramm zum Organisationsverhalten aktiviert werden sollen. Siehe [the section called “Mitgliedskonten von Organisationen verwalten”](#).

Auf der Seite Konten werden dem Detective-Administratorkonto alle Konten der Organisation angezeigt.

Wenn das Detective-Administratorkonto bereits das Administratorkonto für ein Verhaltensdiagramm war, wird dieses Verhaltensdiagramm zum Verhaltensdiagramm der Organisation. Organisationskonten, die in diesem Verhaltensdiagramm bereits Mitgliedskonten waren, werden automatisch als Mitgliedskonten aktiviert. Andere Organisationskonten haben den Status Kein Mitglied.

Organisationskonten haben den Typ Nach Organisation, auch wenn es sich zuvor um Mitgliedskonten auf Einladung handelte.

Mitgliedskonten, die nicht zur Organisation gehören, haben den Typ Auf Einladung.

Auf der Seite Kontoverwaltung steht außerdem die Option Neue Organisationskonten automatisch aktivieren zur Verfügung, mit der neue Konten automatisch aktiviert werden, wenn sie einer Organisation hinzugefügt werden. Siehe [the section called “Neue Organisationskonten automatisch aktivieren”](#). Die Option ist zunächst deaktiviert.

Wenn das Detective-Administratorkonto zum ersten Mal die Kontoverwaltungsseite anzeigt, wird eine Meldung mit der Schaltfläche Alle Organisationskonten aktivieren eingeblendet. Wenn Sie Alle Organisationskonten aktivieren wählen, führt Detective die folgenden Aktionen aus:

- Aktiviert alle aktuellen Organisationskonten als Mitgliedskonten.
- Aktiviert die Option zum automatischen Aktivieren neuer Organisationskonten.

In der Liste der Mitgliedskonten gibt es auch die Option Alle Organisationskonten aktivieren.

Festlegen des Detective-Administratorkontos für eine Organisation

Im Verhaltensdiagramm der Organisation verwaltet das Detective-Administratorkonto die Mitgliedschaft im Verhaltensdiagramm für alle Organisationskonten.

So wird das Detective-Administratorkonto verwaltet

Das Organisationsverwaltungskonto bestimmt das Detective-Administratorkonto für die jeweilige Organisation. AWS-Region

Das Detective-Administratorkonto als delegiertes Administratorkonto einrichten

Das Detective-Administratorkonto wird auch zum delegierten Administratorkonto für Detective in AWS Organizations. Die Ausnahme ist, wenn sich das Verwaltungskonto der Organisation selbst als Detective-Administratorkonto ausgibt. Das Organisationsmanagementkonto kann kein delegierter Administrator in Organizations sein.

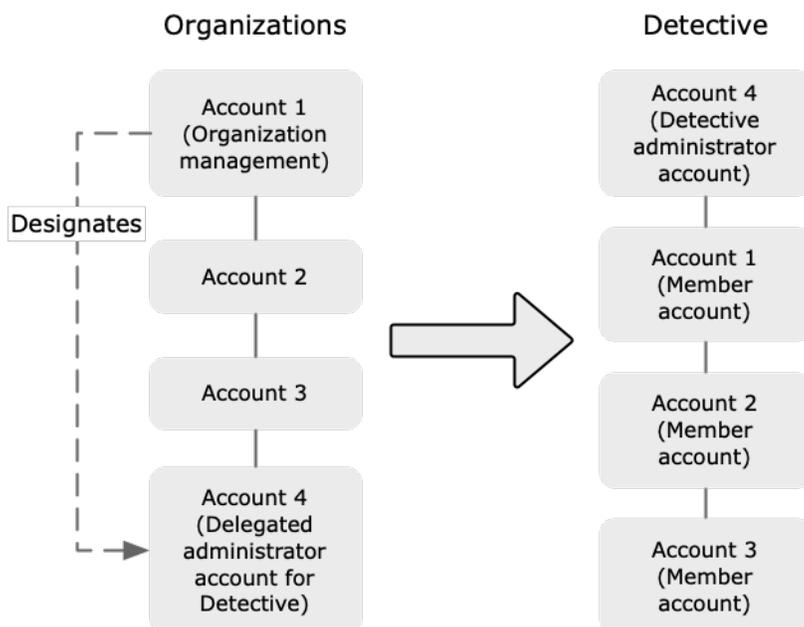
Nachdem das delegierte Administratorkonto in Organizations eingerichtet wurde, kann das Verwaltungskonto der Organisation nur entweder das delegierte Administratorkonto oder ihr eigenes Konto als Detective-Administratorkonto auswählen. Wir empfehlen, dass Sie in allen Regionen das delegierte Administratorkonto wählen.

Das Verhaltensdiagramm der Organisation erstellen und verwalten

Wenn das Verwaltungskonto der Organisation ein Detective-Administratorkonto auswählt, erstellt Detective ein neues Verhaltensdiagramm für dieses Konto. Dieses Verhaltensdiagramm ist das Verhaltensdiagramm der Organisation.

Wenn das Detective-Administratorkonto ein Administratorkonto für ein vorhandenes Verhaltensdiagramm ist, wird dieses Verhaltensdiagramm zum Verhaltensdiagramm der Organisation.

Das Detective Administratorkonto wählt Organisationskonten aus, die als Mitgliedskonten im Diagramm zum Organisationsverhalten aktiviert werden sollen.



Das Detective-Administratorkonto kann auch Einladungen an Konten senden, die nicht zur Organisation gehören. Weitere Informationen finden Sie unter [the section called “Mitgliedskonten von Organisationen verwalten”](#) und [the section called “Verwaltung eingeladener Konten”](#).

Entfernen des Detective-Administratorkontos

Das Verwaltungskonto der Organisation kann das aktuelle Detective-Administratorkonto in einer Region entfernen. Wenn Sie das Detective-Administratorkonto entfernen, entfernt Detective es nur aus der aktuellen Region. Das delegierte Administratorkonto in Organizations wird dadurch nicht geändert.

Wenn das Verwaltungskonto der Organisation das Detective-Administratorkonto in einer Region entfernt, löscht Detective das Verhaltensdiagramm der Organisation. Detective ist für das entfernte Detective-Administratorkonto deaktiviert.

Um das aktuelle delegierte Administratorkonto für Detective zu entfernen, verwenden Sie die Organizations API. Wenn Sie das delegierte Administratorkonto für Detective in Organizations entfernen, löscht Detective alle Diagramme zum Organisationsverhalten, in denen das delegierte Administratorkonto das Detective-Administratorkonto ist. Verhaltensdiagramme von Organisationen, bei denen das Verwaltungskonto der Organisation das Detective-Administratorkonto ist, sind nicht betroffen.

Erforderliche Berechtigungen zur Konfiguration des Detective-Administratorkontos

Um sicherzustellen, dass das Verwaltungskonto der Organisation das Detective-Administratorkonto konfigurieren kann, können Sie die [AmazonDetectiveOrganizationsAccessverwaltete Richtlinie](#) an Ihre AWS Identity and Access Management (IAM)-Entitäten anhängen.

Festlegen eines Detective-Administratorkontos (Konsole)

Das Verwaltungskonto der Organisation kann die Detective-Konsole verwenden, um das Detective-Administratorkonto festzulegen.

Sie müssen Detective nicht aktivieren, um das Detective-Administratorkonto zu verwalten. Sie können das Detective-Administratorkonto auf der Seite Detective aktivieren verwalten.

So legen Sie ein Detective-Administratorkonto fest (Seite Detective aktivieren)

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.

2. Wählen Sie Erste Schritte aus.
3. Erteilen Sie im Bereich Erforderliche Berechtigungen für Administratorkonten dem ausgewählten Konto die erforderlichen Berechtigungen, damit es als Detective-Administrator mit vollem Zugriff auf alle Aktionen in Detective agieren kann. Wenn Sie als Administrator arbeiten möchten, empfehlen wir, die `AmazonDetectiveFullAccess`-Richtlinie dem Prinzipal zuzuordnen.
4. Wählen Sie Richtlinie von IAM anhängen, um die empfohlene Richtlinie direkt in der IAM-Konsole anzuzeigen.
5. Gehen Sie je nachdem, ob Sie über Berechtigungen in der IAM-Konsole verfügen, wie folgt vor:
 - Wenn Sie über Berechtigungen für den Betrieb in der IAM-Konsole verfügen, fügen Sie dem Prinzipal, den Sie für Detective verwenden, die empfohlene Richtlinie hinzu.
 - Wenn Sie nicht über Berechtigungen zum Arbeiten in der IAM-Konsole verfügen, kopieren Sie den Amazon-Ressourcennamen (ARN) der Richtlinie und geben Sie ihn Ihrem IAM-Administrator. Er kann die Richtlinie dann in Ihrem Namen anhängen.
6. Wählen Sie unter Delegierter Administrator das Detective-Administratorkonto aus.

Die verfügbaren Optionen hängen davon ab, ob Sie über ein delegiertes Administratorkonto für Detective in Organizations verfügen.

- Wenn Sie kein delegiertes Administratorkonto für Detective in Organizations haben, geben Sie die Konto-ID des Kontos ein, um es als Detective-Administratorkonto zu kennzeichnen.

Möglicherweise verfügen Sie bereits über ein Administratorkonto und ein Verhaltensdiagramm aus dem manuellen Einladungsprozess. In diesem Fall empfehlen wir, dass Sie dieses Konto als Detective-Administratorkonto festlegen.

Wenn Sie ein delegiertes Administratorkonto in Organizations for Amazon GuardDuty oder Amazon Macie haben, fordert Detective Sie auf, eines dieser Konten auszuwählen. AWS Security Hub Sie können auch ein anderes Konto eingeben.

- Wenn Sie über ein delegiertes Administratorkonto für Detective in Organizations verfügen, werden Sie aufgefordert, entweder dieses Konto oder Ihr Konto auszuwählen. Wir empfehlen, dass Sie in allen Regionen das delegierte Administratorkonto wählen.

7. Wählen Sie Delegieren.

Wenn Sie Detective aktiviert haben oder ein Mitgliedskonto in einem vorhandenen Verhaltensdiagramm sind, können Sie das Detective-Administratorkonto auf der Seite Allgemein festlegen.

So legen Sie ein Detective-Administratorkonto fest (Seite Allgemein)

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Klicken Sie im Detective-Navigationsbereich unter Einstellungen auf Allgemein.
3. Im Bereich Verwaltete Richtlinien können Sie mehr über alle verwalteten Richtlinien erfahren, die Detective unterstützt. Sie können einem Konto die erforderlichen Berechtigungen gewähren, je nachdem, welche Aktionen Benutzer in Detective ausführen sollen. Wenn Sie als Administrator arbeiten möchten, empfehlen wir, die AmazonDetectiveFullAccess-Richtlinie dem Prinzipal zuzuordnen.
4. Gehen Sie je nachdem, ob Sie über Berechtigungen in der IAM-Konsole verfügen, wie folgt vor:
 - Wenn Sie über Berechtigungen für den Betrieb in der IAM-Konsole verfügen, fügen Sie dem Prinzipal, den Sie für Detective verwenden, die empfohlene Richtlinie hinzu.
 - Wenn Sie nicht über Berechtigungen zum Arbeiten in der IAM-Konsole verfügen, kopieren Sie den Amazon-Ressourcennamen (ARN) der Richtlinie und geben Sie ihn Ihrem IAM-Administrator. Er kann die Richtlinie dann in Ihrem Namen anhängen.

Die verfügbaren Optionen hängen davon ab, ob Sie über ein delegiertes Administratorkonto für Detective in Organizations verfügen.

- Wenn Sie kein delegiertes Administratorkonto für Detective in Organizations haben, geben Sie die Konto-ID des Kontos ein, um es als Detective-Administratorkonto zu kennzeichnen.

Möglicherweise verfügen Sie bereits über ein Administratorkonto und ein Verhaltensdiagramm aus dem manuellen Einladungsprozess. In diesem Fall empfehlen wir, dass Sie dieses Konto als Detective-Administratorkonto festlegen.

Wenn Sie ein delegiertes Administratorkonto in Organizations for Amazon GuardDuty oder Amazon Macie haben, fordert Detective Sie auf, eines dieser Konten auszuwählen. AWS Security Hub Sie können auch ein anderes Konto eingeben.

- Wenn Sie über ein delegiertes Administratorkonto für Detective in Organizations verfügen, werden Sie aufgefordert, entweder dieses Konto oder Ihr Konto auszuwählen. Wir empfehlen, dass Sie in allen Regionen das delegierte Administratorkonto wählen.

5. Wählen Sie Delegieren.

Benennen eines Detective-Administratorkontos (Detective API, AWS CLI)

Um das Detective-Administratorkonto festzulegen, können Sie einen API-Aufruf oder die AWS Command Line Interface verwenden. Sie müssen die Anmeldedaten für das Verwaltungskonto der Organisation verwenden.

Wenn Sie bereits über ein delegiertes Administratorkonto für Detective in Organisationen verfügen, müssen Sie entweder dieses Konto oder Ihr Konto auswählen. Wir empfehlen Ihnen, das delegierte Administratorkonto zu wählen.

Um das Detective-Administratorkonto festzulegen (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [EnableOrganizationAdminAccount](#). Sie müssen die AWS -Konto-ID des Detective-Administratorkontos angeben. Verwenden Sie die Operation [ListOrganizationAdminAccounts](#), um die Konto-ID abzurufen.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl [enable-organization-admin-account](#) aus.

```
aws detective enable-organization-admin-account --account-id <admin account ID>
```

Beispiel

```
aws detective enable-organization-admin-account --account-id 777788889999
```

Entfernen eines Detective-Administratorkontos (Konsole)

Von der Detective-Konsole aus können Sie das Detective-Administratorkonto entfernen.

Wenn Sie das Detective-Administratorkonto entfernen, wird Detective für das Konto deaktiviert und das Verhaltensdiagramm der Organisation wird gelöscht. Das Detective Administratorkonto wird nur in der aktuellen Region entfernt.

 **Important**

Das Entfernen eines Detective-Administratorkontos hat keine Auswirkungen auf das delegierte Administratorkonto in Organizations.

So entfernen Sie das Detective-Administratorkonto (Seite Detective aktivieren)

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie Erste Schritte aus.
3. Wählen Sie unter Delegierter Administrator die Option Amazon Detective deaktivieren aus.
4. Geben Sie im Bestätigungsdialogfeld **disable** ein, und wählen Sie dann Amazon Detective deaktivieren.

So entfernen Sie ein Detective-Administratorkonto (Seite Allgemein)

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Klicken Sie im Detective-Navigationsbereich unter Einstellungen auf Allgemein.
3. Wählen Sie unter Delegierter Administrator die Option Amazon Detective deaktivieren aus.
4. Geben Sie im Bestätigungsdialogfeld **disable** ein, und wählen Sie dann Amazon Detective deaktivieren.

Das Detective-Administratorkonto entfernen (Detective API, AWS CLI)

Um das Detective-Administratorkonto zu entfernen, können Sie einen API-Aufruf oder die AWS CLI verwenden. Sie müssen die Anmeldedaten für das Verwaltungskonto der Organisation verwenden.

Wenn Sie das Detective-Administratorkonto entfernen, wird Detective für das Konto deaktiviert und das Verhaltensdiagramm der Organisation wird gelöscht.

 **Important**

Das Entfernen eines Detective-Administratorkontos hat keine Auswirkungen auf das delegierte Administratorkonto in Organizations.

Um das Detective-Administratorkonto zu entfernen (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [DisableOrganizationAdminAccount](#).

Wenn Sie die Detective-API verwenden, um das Detective-Administratorkonto zu entfernen, wird es nur in der Region entfernt, in der der API-Aufruf oder -Befehl ausgeführt wurde.

- AWS CLI: Führen Sie in der Befehlszeile den Befehl [disable-organization-admin-account](#) aus.

```
aws detective disable-organization-admin-account
```

Das delegierte Administratorkonto entfernen (Organizations API, AWS CLI)

Durch das Entfernen des Detective-Administratorkontos wird das delegierte Administratorkonto in Organizations nicht automatisch entfernt. Um das delegierte Administratorkonto für Detective zu entfernen, können Sie die Organizations API verwenden.

Wenn Sie das delegierte Administratorkonto entfernen, werden dadurch alle Verhaltensdiagramme der Organisation gelöscht, in denen das delegierte Administratorkonto das Detective-Administratorkonto ist. Außerdem wird Detective für das Konto in diesen Regionen deaktiviert.

Um das delegierte Administratorkonto zu entfernen (Organizations API, AWS CLI)

- Organizations-API: Verwenden Sie die Operation [DeregisterDelegatedAdministrator](#). Sie müssen die Konto-ID des Detective-Administratorkontos und den Dienstprinzipal für Detective angeben, nämlich `detective.amazonaws.com`.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl [deregister-delegated-administrator](#) aus.

```
aws organizations deregister-delegated-administrator --account-id <Detective administrator account ID> --service-principal <Detective service principal>
```

Beispiel

```
aws organizations deregister-delegated-administrator --account-id 777788889999 --service-principal detective.amazonaws.com
```

Verfügbare Aktionen für Konten

Administrator- und Mitgliedskonten haben Zugriff auf die folgenden Detective-Aktionen. In der Tabelle haben die Werte die folgenden Bedeutungen:

- **Beliebig** – Das Konto kann die Aktion für alle Konten unter demselben Detective-Administratorkonto ausführen.
- **Selbst** – Das Konto kann die Aktion nur für sein eigenes Konto ausführen.
- **Strich (-)** – Das Konto kann die Aktion nicht ausführen.

Im Diagramm zum Organisationsverhalten bestimmt das Detective-Administratorkonto, welche Organisationskonten als Mitgliedskonten aktiviert werden sollen. Detective kann so konfiguriert werden, dass neue Organisationskonten automatisch als Mitgliedskonten aktiviert werden, oder sie können Organisationskonten auch manuell aktivieren.

Ein Administratorkonto kann Konten dazu einladen, Mitgliedskonten im Verhaltensdiagramm zu werden. Wenn ein Mitgliedskonto die Einladung annimmt und aktiviert ist, beginnt Amazon Detective, die Daten des Mitgliedskontos aufzunehmen und in dieses Verhaltensdiagramm zu extrahieren.

Bei anderen Verhaltensdiagrammen als dem Verhaltensdiagramm der Organisation handelt es sich bei allen Mitgliedskonten um eingeladene Konten.

Die folgende Tabelle zeigt die Standardberechtigungen für Administrator- und Mitgliedskonten. Sie können benutzerdefinierte IAM-Richtlinien verwenden, um den Zugriff auf die Features und Funktionen von Detective weiter einzuschränken.

Aktion	Administratorkonto (Organisation)	Administratorkonto (Einladung)	Mitglied (Organisation)	Mitglied (Einladung)
Konten anzeigen	Any	Any	Selbst (Administratorkonten anzeigen)	Selbst (Administratorkonten anzeigen)
Mitgliedskonto entfernen	Any	Any	-	Selbst

Aktion	Administratorkonto (Organisation)	Administratorkonto (Einladung)	Mitglied (Organisation)	Mitglied (Einladung)
	Eingeladene Konten werden entfernt Organisationskonten werden getrennt			
Optionale Datenquellenpakete hinzufügen oder entfernen	Beliebig (Die Einstellung gilt für alle Mitgliedskonten)	Beliebig (Die Einstellung gilt für alle Mitgliedskonten)	–	–
Detective deaktivieren	Selbst	Selbst	–	–
Verhalten sdiagrammdateien anzeigen	Any	Any	–	–
Aktivieren oder deaktivieren optionaler Datenquellenpakete	Alle	Alle	–	–

Anzeige der Kontenliste

Das Administratorkonto kann die Detective-Konsole oder die API verwenden, um eine Liste von Konten anzuzeigen. Die Liste kann Folgendes beinhalten:

- Konten, die das Administratorkonto zum Beitritt zum Verhaltensdiagramm eingeladen hat. Diese Konten haben den Typ Auf Einladung.

- Für das Organisationsverhaltensdiagramm alle Konten in der Organisation. Diese Konten haben den Typ Nach Organisation.

In den Erkenntnissen sind Konten eingeladener Mitglieder, die eine Einladung abgelehnt haben oder die das Administratorkonto aus dem Verhaltensdiagramm entfernt hat, nicht enthalten. Sie umfassen nur Konten mit den folgenden Status.

Überprüfung im Gange

Bei eingeladenen Konten überprüft Detective die E-Mail-Adresse des Kontos, bevor die Einladung gesendet wird.

Bei Organisationskonten überprüft Detective, ob das Konto der Organisation gehört. Detective überprüft auch, ob es das Detective-Administratorkonto war, das das Konto aktiviert hat.

Überprüfung fehlgeschlagen

Die Überprüfung ist fehlgeschlagen. Die Einladung wurde nicht gesendet, oder das Organisationskonto wurde nicht als Mitglied aktiviert.

Eingeladen

Für eingeladene Konten. Die Einladung wurde gesendet, aber das Mitgliedskonto hat noch nicht geantwortet.

Kein Mitglied

Für Organisationskonten im Verhaltensdiagramm der Organisation. Das Organisationskonto ist derzeit kein Mitgliedskonto. Es trägt keine Daten zum Verhaltensdiagramm der Organisation bei.

Aktiviert

Bei Konten mit Einladung hat das Mitgliedskonto die Einladung angenommen und trägt Daten zum Verhaltensdiagramm bei.

Für Organisationskonten im Diagramm zum Organisationsverhalten hat das Detective-Administratorkonto das Konto als Mitgliedskonto aktiviert. Das Konto trägt Daten zum Verhaltensdiagramm der Organisation bei.

Nicht aktiviert

Bei Konten mit Einladung hat das Mitgliedskonto die Einladung akzeptiert, sie kann aber nicht aktiviert werden.

Für Organisationskonten im Diagramm zum Organisationsverhalten hat das Detective-Administratorkonto versucht, das Konto zu aktivieren, aber das Konto kann nicht aktiviert werden.

Dieser Status kann aus folgenden Gründen auftreten:

- Das Mitgliedskonto war seit mindestens 48 Stunden kein GuardDuty Amazon-Kunde mehr.
- Die Daten des Mitgliedskontos würden dazu führen, dass das Datenvolumen des Verhaltensdiagramms das Detective-Kontingent überschreitet.

Auflisten von Konten (Konsole)

Sie können den verwenden AWS Management Console , um Ihre Kontoliste einzusehen und zu filtern.

So zeigen Sie die Liste der Konten an (Konsole)

1. Melden Sie sich bei der an AWS Management Console. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich von Detective Zugriffsverwaltung aus.

Die Liste der Mitgliedskonten enthält die folgenden Konten:

- Ihr Konto
- Konten, die Sie eingeladen haben, Daten zum Verhaltensdiagramm beizutragen
- Im Verhaltensdiagramm der Organisation sind alle Unternehmenskonten aufgeführt.

Für jedes Konto zeigt die Liste die folgenden Informationen an:

- Die AWS Konto-ID.
- Bei Organisationskonten der Kontoname.
- Der Kontotyp (Auf Einladung oder Nach Organisation).
- Bei eingeladenen Konten die E-Mail-Adresse des Root-Benutzers des Kontos.
- Der Kontostatus.
- Das tägliche Datenvolumen für das Konto. Detective kann das Datenvolumen für Konten, die nicht als Mitgliedskonten aktiviert sind, nicht abrufen.
- Das Datum, an dem der Kontostatus zuletzt aktualisiert wurde.

Sie können die Reiter oben in der Tabelle verwenden, um die Liste nach dem Status des Mitgliedskontos zu filtern. Auf jedem Reiter wird die Anzahl der passenden Mitgliedskonten angezeigt.

- Klicken Sie auf Alle, um alle Mitgliedskonten anzuzeigen.
- Wählen Sie Aktiviert, um Konten mit dem Status Aktiviert anzuzeigen.
- Wählen Sie Nicht aktiviert, um Konten mit einem anderen Status als Aktiviert anzuzeigen.

Sie können der Liste der Mitgliedskonten auch andere Filter hinzufügen.

So fügen Sie der Liste der Konten im Verhaltensdiagramm (Konsole) einen Filter hinzu

1. Wählen Sie das Filterfeld.
2. Wählen Sie die Spalte, nach der Sie die Liste filtern möchten.
3. Wählen Sie für die angegebene Spalte den Wert aus, der für den Filter verwendet werden soll.
4. Um einen Filter zu entfernen, wählen Sie das X-Symbol oben rechts.
5. Klicken Sie auf das Symbol „Aktualisieren“ oben rechts, um die Liste mit den aktuellen Statusinformationen zu aktualisieren.

Deine Mitgliedskonten auflisten (Detective API, AWS CLI)

Sie können einen API-Aufruf oder die verwenden AWS Command Line Interface , um eine Liste der Mitgliedskonten in Ihrem Verhaltensdiagramm anzuzeigen.

Verwenden Sie die Operation [ListGraphs](#), um den ARN Ihres Verhaltensdiagramms zur Verwendung in der Anfrage abzurufen.

Um eine Liste von Mitgliedskonten abzurufen (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [ListMembers](#). Um das beabsichtigte Verhaltensdiagramm zu identifizieren, geben Sie den Verhaltensdiagramm-ARN an.

Beachten Sie, dass für das Verhaltensdiagramm der Organisation [ListMembers](#) keine Organisationskonten zurückgibt, die Sie nicht als Mitgliedskonten aktiviert haben oder die Sie vom Verhaltensdiagramm getrennt haben.

- AWS CLI: Führen Sie in der Befehlszeile den Befehl [list-members](#) aus.

```
aws detective list-members --graph-arn <behavior graph ARN>
```

Beispiel:

```
aws detective list-members --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

So rufen Sie Details zu bestimmten Mitgliedskonten in Ihrem Verhaltensdiagramm ab (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [GetMembers](#). Geben Sie den ARN des Verhaltensdiagramms und die Liste der Kontokennungen für die Mitgliedskonten an.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl [get-members](#) aus.

```
aws detective get-members --account-ids <member account IDs> --graph-arn <behavior graph ARN>
```

Beispiel:

```
aws detective get-members --account-ids 444455556666 123456789012 --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Organisationskonten als Mitgliedskonten verwalten

Im Diagramm zum Organisationsverhalten bestimmt das Detective-Administratorkonto, welche Organisationskonten als Mitgliedskonten aktiviert werden sollen.

Detective kann so konfiguriert werden, dass neue Organisationskonten automatisch als Mitgliedskonten aktiviert werden, oder sie können Organisationskonten auch manuell aktivieren.

Das Detective-Administratorkonto kann auch die Zuordnung von Organisationskonten zum Verhaltensdiagramm der Organisation trennen.

Inhalt

- [Neue Organisationskonten automatisch als Mitgliedskonten aktivieren](#)
- [Organisationskonten als Mitgliedskonten aktivieren](#)
- [Aufheben der Zuordnung von Unternehmenskonten zu Mitgliedskonten](#)

Neue Organisationskonten automatisch als Mitgliedskonten aktivieren

Das Detective-Administratorkonto kann Detective so konfigurieren, dass neue Organisationskonten automatisch als Mitgliedskonten im Verhaltensdiagramm der Organisation aktiviert werden.

Wenn Ihrer Organisation neue Konten hinzugefügt werden, werden sie der Liste auf der Kontoverwaltungsseite hinzugefügt. Für Organisationskonten lautet Typ auf Nach Organisation.

Standardmäßig sind neue Organisationskonten nicht als Mitgliedskonten aktiviert. Ihr Status ist Kein Mitglied.

Wenn Sie Organisationskonten automatisch aktivieren möchten, beginnt Detective, neue Konten als Mitgliedskonten zu aktivieren, wenn sie der Organisation hinzugefügt werden. Detective aktiviert keine vorhandenen Organisationskonten, die noch nicht aktiviert sind.

Ob Detective Organisationskonten als Mitgliedskonten aktivieren kann, hängt von den folgenden Faktoren ab:

- Die maximale Anzahl von Mitgliedskonten für ein Verhaltensdiagramm beträgt 1.200. Wenn Ihr Verhaltensdiagramm bereits 1.200 Mitgliedskonten enthält, können keine neuen Konten aktiviert werden.
- Detective kann kein Konto aktivieren, für das Amazon seit mindestens 48 Stunden nicht GuardDuty aktiviert ist.
- Detective kann ein Konto nicht aktivieren, wenn dies dazu führen würde, dass das Datenvolumen des Verhaltensdiagramms den zulässigen Höchstwert überschreitet.

Neue Organisationskonten automatisch aktivieren (Konsole)

Auf der Seite Kontoverwaltung bestimmt die Einstellung Neue Organisationskonten automatisch aktivieren, ob Konten automatisch aktiviert werden, wenn sie einer Organisation hinzugefügt werden.

So aktivieren Sie neue Organisationskonten automatisch als Mitgliedskonten

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich von Detective Zugriffsverwaltung aus.
3. Aktivieren Sie die Option Neue Unternehmenskonten automatisch aktivieren.

Automatisches Aktivieren neuer Organisationskonten (Detective API, AWS CLI)

Um zu bestimmen, ob neue Organisationskonten automatisch als Mitgliedskonten aktiviert werden sollen, kann das Administratorkonto die Detective API oder die AWS Command Line Interface verwenden.

Um die Konfiguration anzuzeigen und zu verwalten, müssen Sie den ARN für das Verhaltensdiagramm angeben. Verwenden Sie die Operation [ListGraphs](#), um den ARN zu erhalten.

So zeigen Sie die aktuelle Konfiguration für die automatische Aktivierung von Organisationskonten an

- Detective API: Verwenden Sie die Operation [DescribeOrganizationConfiguration](#).

In der Antwort heißt es: Wenn neue Organisationskonten automatisch aktiviert werden, dann ist `AutoEnable true`.

- AWS CLI: Führen Sie in der Befehlszeile den Befehl [describe-organization-configuration](#) aus.

```
aws detective describe-organization-configuration --graph-arn <behavior graph ARN>
```

Beispiel

```
aws detective describe-organization-configuration --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

So aktivieren Sie neue Organisationskonten automatisch

- Detective API: Verwenden Sie die Operation [UpdateOrganizationConfiguration](#). Um neue Organisationskonten automatisch zu aktivieren, setzen Sie `AutoEnable auftrue`.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl [update-organization-configuration](#) aus.

```
aws detective update-organization-configuration --graph-arn <behavior graph ARN> --auto-enable | --no-auto-enable
```

Beispiel

```
aws detective update-organization-configuration --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 --auto-enable
```

Organisationskonten als Mitgliedskonten aktivieren

Wenn Sie neue Organisationskonten nicht automatisch aktivieren, können Sie diese Konten manuell aktivieren. Sie müssen Konten, deren Verknüpfung Sie aufgehoben haben, auch manuell aktivieren.

Feststellen, ob ein Konto aktiviert werden kann

Sie können ein Organisationskonto nicht als Mitgliedskonto aktivieren, wenn das Verhaltensdiagramm der Organisation bereits die maximal 1.200 aktivierten Konten enthält. In diesem Fall bleibt der Status des Organisationskontos Kein Mitglied.

Wenn Sie ein Unternehmenskonto aktivieren, überprüft Detective, ob das Konto seit mindestens 48 Stunden GuardDuty Amazon-Kunde ist. Ist dies der Fall, überprüft Detective, ob die Kontodaten dazu führen würden, dass die Datenrate für das Verhaltensdiagramm das Kontingent überschreitet. Diese Überprüfung kann 24 bis 48 Stunden dauern.

Während Detective die Datenrate überprüft, lautet der Status des Mitgliedskontos Nicht aktiviert.

Wenn das Mitgliedskonto beide Prüfungen besteht, wird der Status des Mitgliedskontos auf Aktiviert aktualisiert. Detective beginnt, Daten aus dem Mitgliedskonto in das Verhaltensdiagramm aufzunehmen.

Wenn das Konto eine dieser Prüfungen nicht besteht, bleibt der Status des Mitgliedskontos weiterhin Nicht aktiviert. Das Konto trägt keine Daten zum Verhaltensdiagramm bei.

Sobald das Mitgliedskonto aktiviert werden kann, ändert Detective den Status des Mitgliedskontos automatisch auf Aktiviert.

Organisationskonten als Mitgliedskonten aktivieren (Konsole)

Auf der Kontoverwaltungsseite können Sie Organisationskonten als Mitgliedskonten aktivieren.

So aktivieren Sie Organisationskonten als Mitgliedskonten

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.

2. Wählen Sie im Navigationsbereich von Detective Zugriffsverwaltung aus.
3. Um die Liste der Konten anzuzeigen, die derzeit nicht aktiviert sind, wählen Sie Nicht aktiviert.
4. Sie können entweder bestimmte Organisationskonten auswählen oder alle Organisationskonten aktivieren.

Um ausgewählte Organisationskonten zu aktivieren:

- a. Wählen Sie jedes Organisationskonto aus, das Sie aktivieren möchten.
- b. Wählen Sie Konten aktivieren.

Um alle Organisationskonten zu aktivieren, wählen Sie Alle Organisationskonten aktivieren aus.

Organisationskonten als Mitgliedskonten aktivieren (Detective API, AWS CLI)

Sie können die Detective API oder die verwenden AWS Command Line Interface , um Organisationskonten als Mitgliedskonten im Organisationsverhaltensdiagramm zu aktivieren. Verwenden Sie die Operation [ListGraphs](#), um den ARN Ihres Verhaltensdiagramms zur Verwendung in der Anfrage abzurufen.

Um Organisationskonten als Mitgliedskonten zu aktivieren (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [CreateMembers](#). Sie müssen den Diagramm-ARN angeben.

Geben Sie für jedes Konto die Konto-ID an. Organizations-Konten im Verhaltensdiagramm der Organisation erhalten keine Einladung. Sie müssen keine E-Mail-Adresse oder andere Einladungsinformationen angeben.

- AWS CLI: Führen Sie in der Befehlszeile den Befehl [create-members](#) aus.

```
aws detective create-members --accounts AccountId=<AWS account ID> --graph-arn <behavior graph ARN>
```

Beispiel

```
aws detective create-members --accounts AccountId=444455556666 AccountId=123456789012 --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Aufheben der Zuordnung von Unternehmenskonten zu Mitgliedskonten

Um zu verhindern, dass Daten aus einem Organisationskonto in das Verhaltensdiagramm einer Organisation aufgenommen werden, können Sie die Zuordnung des Kontos aufheben. Bestehende Daten für dieses Konto verbleiben im Verhaltensdiagramm.

Wenn Sie die Zuordnung zu einem Organisationskonto aufheben, ändert sich der Status in Kein Mitglied. Detective hört auf, Daten von diesem Konto aufzunehmen, aber das Konto bleibt in der Liste.

Aufheben der Zuordnung von Organisationskonten (Konsole)

Auf der Kontoverwaltungsseite können Sie die Zuordnung von Organisationskonten als Mitgliedskonten aufheben.

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich von Detective Zugriffsverwaltung aus.
3. Um die Liste der aktivierten Konten anzuzeigen, wählen Sie Aktiviert.
4. Aktivieren Sie das Kontrollkästchen für jedes zu löschende Konto.
5. Wählen Sie Aktionen. Wählen Sie dann Konten deaktivieren.

Der Kontostatus für die getrennten Konten ändert sich in Kein Mitglied.

Organisationskonten trennen (Detective API,) AWS CLI

Sie können die Detective API oder die verwenden AWS Command Line Interface , um Organisationskonten in Ihrem Verhaltensdiagramm als Mitgliedskonten zu trennen.

Verwenden Sie die Operation [ListGraphs](#), um den ARN Ihres Verhaltensdiagramms zur Verwendung in der Anfrage abzurufen.

So heben Sie die Zuordnung von Organisationskonten zum Verhaltensdiagramm der Organisation auf (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [DeleteMembers](#). Geben Sie den Grafik-ARN und die Liste der Kontokennungen für die Mitgliedskonten an, deren Zuordnung aufgehoben werden soll.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl [delete-members](#) aus.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
graph ARN>
```

Beispiel

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Mitgliedskonten eingeladener Mitglieder verwalten

Ein Administratorkonto kann Konten dazu einladen, Mitgliedskonten im Verhaltensdiagramm zu werden. Wenn ein Mitgliedskonto die Einladung annimmt und aktiviert ist, beginnt Amazon Detective, die Daten des Mitgliedskontos aufzunehmen und in dieses Verhaltensdiagramm zu extrahieren.

Bei anderen Verhaltensdiagrammen als dem Verhaltensdiagramm der Organisation handelt es sich bei allen Mitgliedskonten um eingeladene Konten.

Das Detective-Administratorkonto kann auch Konten, die keine Organisationskonten sind, in das Verhaltensdiagramm der Organisation einladen.

Das Administratorkonto kann Mitgliedskonten aus dem Verhaltensdiagramm entfernen.

Inhalt

- [Mitgliedskonten zu einem Verhaltensdiagramm einladen](#)
- [Aktivierung eines Mitgliedskontos, das nicht aktiviert ist](#)
- [Mitgliedskonten aus einem Verhaltensdiagramm entfernen](#)

Mitgliedskonten zu einem Verhaltensdiagramm einladen

Das Administratorkonto kann Konten einladen, zu einem Verhaltensdiagramm beizutragen. Ein Verhaltensdiagramm kann bis zu 1.200 Mitgliedskonten enthalten.

Auf oberster Ebene sieht das Verfahren zum Einladen von Konten zur Mitwirkung an einem Verhaltensdiagramm wie folgt aus.

1. Für jedes Mitgliedskonto, das hinzugefügt werden soll, gibt das AWS Administratorkonto die Konto-ID und die E-Mail-Adresse des Root-Benutzers an.

2. Detective bestätigt, dass die E-Mail-Adresse die E-Mail-Adresse des Stammbenutzers für das Konto ist.

Detective führt diese Überprüfung nicht in den Regionen AWS GovCloud (USA-Ost) oder AWS GovCloud (US-West) durch.

3. Wenn die Kontoinformationen gültig sind, sendet Detective die Einladung an das Mitgliedskonto.

Detective sendet niemals E-Mail-Einladungen an Mitgliedskonten in den AWS GovCloud Regionen (USA-Ost) oder AWS GovCloud (US-West).

Für andere Regionen bietet die Detective API die Option, keine Einladungen an die Mitgliedskonten zu senden.

Diese Option ist nützlich für Konten, die zentral verwaltet werden.

4. Das Mitgliedskonto akzeptiert oder lehnt die Einladung ab.

Auch wenn das Administratorkonto keine Einladungs-E-Mails versendet, muss das Mitgliedskonto dennoch auf die Einladung antworten.

5. Wenn das Mitgliedskonto die Einladung annimmt, überprüft Detective, ob das Mitgliedskonto seit mindestens 48 Stunden GuardDuty Amazon-Kunde ist.

Ist dies der Fall, überprüft Detective, ob die Daten des Mitgliedskontos dazu führen würden, dass die Datenrate für das Verhaltensdiagramm das Kontingent überschreitet.

Diese Überprüfung kann zwischen 24 und 48 Stunden dauern.

Während Detective die Datenrate überprüft, lautet der Status des Mitgliedskontos Nicht aktiviert.

6. Wenn das Mitgliedskonto beide Prüfungen besteht, wird der Status des Mitgliedskontos automatisch auf Aktiviert aktualisiert. Detective beginnt, Daten aus dem Mitgliedskonto in das Verhaltensdiagramm aufzunehmen.

Wenn es eine dieser Prüfungen nicht besteht, bleibt der Status des Mitgliedskontos weiterhin Nicht aktiviert. Das Mitgliedskonto trägt keine Daten zum Verhaltensdiagramm bei.

7. Sobald das Mitgliedskonto aktiviert werden kann, ändert Detective den Status des Mitgliedskontos automatisch auf Aktiviert.

Beispielsweise ändert sich der Status des Mitgliedskontos in Aktiviert, wenn ein Mitgliedskonto aktiviert wird GuardDuty und Detective überprüft, ob sein Datenvolumen nicht zu groß ist, oder wenn das Administratorkonto andere Mitgliedskonten entfernt, um Platz für ein Konto zu schaffen.

Wenn mehr als ein Konto Nicht aktiviert ist, aktiviert Detective die Konten in der Reihenfolge, in der sie eingeladen wurden. Der Prozess zur Überprüfung, ob Konten mit dem Status Nicht aktiviert aktiviert werden sollen, wird stündlich ausgeführt.

Das Administratorkonto kann Konten auch manuell aktivieren, anstatt auf den automatischen Vorgang zu warten. Beispielsweise möchte das Administratorkonto möglicherweise die Konten auswählen, die aktiviert werden sollen. Siehe [the section called “Aktivierung eines Mitgliedskontos, das nicht aktiviert ist”](#).

Beachten Sie, dass Detective am 12. Mai 2021 damit begonnen hat, Konten, die Nicht aktiviert sind, automatisch zu aktivieren. Konten, die zuvor Nicht aktiviert waren, werden nicht automatisch aktiviert. Das Administratorkonto muss sie manuell aktivieren.

Einzelne Konten zu einem Verhaltensdiagramm einladen (Konsole)

Sie können die Mitgliedskonten manuell angeben, die eingeladen werden sollen, ihre Daten zu einem Verhaltensdiagramm beizutragen.

So wählen Sie die Mitgliedskonten, die eingeladen werden sollen, manuell aus (Konsole)

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich von Detective Zugriffsverwaltung aus.
3. Wählen Sie Aktionen. Wählen Sie dann Konten einladen aus.
4. Wählen Sie unter Konten hinzufügen die Option Einzelne Konten hinzufügen aus.
5. Gehen Sie wie folgt vor, um der Einladungsliste ein Mitgliedskonto hinzuzufügen.
 - a. Wählen Sie Konto hinzufügen aus.
 - b. Geben Sie als AWS Konto-ID die AWS Konto-ID ein.
 - c. Geben Sie unter E-Mail-Adresse die E-Mail-Adresse des Root-Benutzers des Kontos ein.
6. Um ein Konto aus der Liste zu entfernen, wählen Sie für dieses Konto Entfernen aus.
7. Fügen Sie unter Einladungs-E-Mail personalisieren benutzerdefinierte Inhalte hinzu, die in die Einladungs-E-Mail aufgenommen werden sollen.

In diesem Bereich können Sie beispielsweise Kontaktinformationen angeben. Oder verwenden Sie ihn, um das Mitgliedskonto daran zu erinnern, dass es seinem Benutzer oder seiner Rolle die erforderliche IAM-Richtlinie zuordnen muss, bevor es die Einladung annehmen kann.

- Die IAM-Richtlinie für Mitgliedskonten enthält den Text der erforderlichen IAM-Richtlinie für Mitgliedskonten. Die E-Mail-Einladung enthält diesen Richtlinientext. Um den Richtlinientext zu kopieren, wählen Sie Kopieren.
- Klicken Sie auf Einladen.

Einladen einer Liste von Mitgliedskonten in ein Verhaltensdiagramm (Konsole)

In der Detective-Konsole können Sie eine .csv-Datei mit einer Liste von Mitgliedskonten bereitstellen, die Sie zu Ihrem Verhaltensdiagramm einladen möchten.

Die erste Zeile in der Datei ist die Kopfzeile. Jedes Konto wird dann in einer separaten Zeile aufgeführt. Jeder Mitgliedskontoeintrag enthält die AWS Konto-ID und die E-Mail-Adresse des Root-Benutzers des Kontos.

Beispiel:

```
Account ID,Email address
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Wenn Detective die Datei verarbeitet, ignoriert es Konten, die bereits eingeladen wurden, es sei denn, der Kontostatus lautet Überprüfung fehlgeschlagen. Dieser Status weist darauf hin, dass die für das Konto angegebene E-Mail-Adresse nicht mit der E-Mail-Adresse des Root-Benutzers des Kontos übereinstimmt. In diesem Fall löscht Detective die ursprüngliche Einladung und versucht erneut, die E-Mail-Adresse zu überprüfen und die Einladung zu versenden.

Diese Option bietet auch eine Vorlage, die Sie verwenden können, um die Kontenliste zu erstellen.

Mitgliedskonten aus einer .csv-Liste (Konsole) einladen

- Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
- Wählen Sie im Navigationsbereich von Detective Zugriffsverwaltung aus.
- Wählen Sie Aktionen. Wählen Sie dann Konten einladen aus.
- Wählen Sie unter Konten hinzufügen die Option Aus CSV-Datei hinzufügen aus.
- Um eine Vorlagendatei herunterzuladen, mit der Sie arbeiten können, wählen Sie CSV-Vorlage herunterladen.
- Um die Datei auszuwählen, die die Liste der Konten enthält, wählen Sie .csv-Datei auswählen.

7. Überprüfen Sie unter Mitgliedskonten überprüfen die Liste der Mitgliedskonten, die Detective in der Datei gefunden hat.
8. Fügen Sie unter Einladungs-E-Mail personalisieren benutzerdefinierte Inhalte hinzu, die in die Einladungs-E-Mail aufgenommen werden sollen.

Sie können beispielsweise Kontaktinformationen angeben oder das Mitgliedskonto an die erforderliche IAM-Richtlinie erinnern.

9. Die IAM-Richtlinie für Mitgliedskonten enthält den Text der erforderlichen IAM-Richtlinie für Mitgliedskonten. Die E-Mail-Einladung enthält diesen Richtlinienentext. Um den Richtlinienentext zu kopieren, wählen Sie Kopieren.
10. Klicken Sie auf Einladen.

Mitgliedskonten zu einem Verhaltensdiagramm einladen (Detective API, AWS CLI)

Sie können die Detective API oder die verwendete AWS Command Line Interface, um Mitgliedskonten einzuladen, ihre Daten zu einem Verhaltensdiagramm beizutragen. Verwenden Sie die Operation [ListGraphs](#), um den ARN Ihres Verhaltensdiagramms zur Verwendung in der Anfrage abzurufen.

Um Mitgliedskonten zu einem Verhaltensdiagramm einzuladen (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [CreateMembers](#). Sie müssen den Diagramm-ARN angeben. Geben Sie für jedes Konto die Konto-ID und die E-Mail-Adresse des Root-Benutzers an.

Um keine Einladungs-E-Mails an die Mitgliedskonten zu senden, setzen Sie den Wert `DisableEmailNotification` auf „true“. Der Standardwert für `DisableEmailNotification` ist „false“.

Wenn Sie Einladungs-E-Mails versenden, können Sie optional einen benutzerdefinierten Text angeben, der der Einladungs-E-Mail hinzugefügt werden soll.

- AWS CLI: Führen Sie in der Befehlszeile den Befehl `create-members` aus.

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root user email address> --graph-arn <behavior graph ARN> --message "<Custom message text>"
```

Beispiel

```
aws detective create-members --accounts
  AccountId=444455556666,EmailAddress=mmajor@example.com
  AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
  arn:aws:detective:us-east-1:111122223333:graph:123412341234 --message "This is Paul
  Santos. I need to add your account to the data we use for security investigation in
  Amazon Detective. If you have any questions, contact me at psantos@example.com."
```

Um anzugeben, dass keine Einladungs-E-Mails an die Mitgliedskonten gesendet werden sollen, fügen Sie `--disable-email-notification` hinzu.

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root
  user email address> --graph-arn <behavior graph ARN> --disable-email-notification
```

Beispiel

```
aws detective create-members --accounts
  AccountId=444455556666,EmailAddress=mmajor@example.com
  AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
  arn:aws:detective:us-east-1:111122223333:graph:123412341234 --disable-email-
  notification
```

Hinzufügen einer Liste von Mitgliedskonten in allen Regionen (Python-Skript aktiviert GitHub)

Detective bietet ein Open-Source-Skript [GitHub](#) , mit dem Sie Folgendes tun können:

- Fügt den Verhaltensdiagrammen eines Administratorkontos in einer bestimmten Liste von Regionen eine bestimmte Liste von Mitgliedskonten hinzu.
- Wenn das Administratorkonto in einer Region kein Verhaltensdiagramm hat, aktiviert das Skript auch Detective und erstellt das Verhaltensdiagramm in dieser Region.
- Senden Sie Einladungs-E-Mails an die Mitgliedskonten.
- Aktivieren Sie die Einladungen für die Mitgliedskonten automatisch.

Informationen zur Konfiguration und Verwendung der GitHub Skripts finden Sie unter [the section called "Amazon Detective Python-Skripte"](#).

Aktivierung eines Mitgliedskontos, das nicht aktiviert ist

Nachdem ein Mitgliedskonto eine Einladung angenommen hat, prüft Amazon Detective, ob das Mitgliedskonto aktiviert werden kann. Wenn Detective das Mitgliedskonto nicht aktivieren kann, wird der Status des Mitgliedskontos auf Nicht aktiviert gesetzt. Dies kann aus einem der folgenden Gründe geschehen.

- Das Mitgliedskonto war seit mindestens 48 Stunden kein GuardDuty Amazon-Kunde mehr.
- Detective überprüft das Datenvolumen für das Mitgliedskonto.
- Die Daten des Mitgliedskontos würden dazu führen, dass die Datenrate des Verhaltensdiagramms das Kontingent überschreitet.

Mitgliedskonten, die Nicht aktiviert sind, tragen keine Daten zum Verhaltensdiagramm bei.

Detective aktiviert Konten automatisch, da das Verhaltensdiagramm sie berücksichtigen kann.

Sie können auch versuchen, Mitgliedskonten manuell zu aktivieren, bei denen es sich um nicht aktivierte Mitgliedskonten handelt. Sie können beispielsweise bestehende Mitgliedskonten entfernen, um das Datenvolumen zu reduzieren. Anstatt auf den automatischen Prozess zur Aktivierung der Konten zu warten, können Sie versuchen, Mitgliedskonten mit dem Status Nicht aktiviert zu aktivieren.

Aktivieren eines Mitgliedskontos, das nicht aktiviert ist (Konsole)

Die Liste der Mitgliedskonten enthält eine Option zum Aktivieren ausgewählter Mitgliedskonten, die Nicht aktiviert sind.

So aktivieren Sie ein Mitgliedskonto, das nicht aktiviert ist

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich von Detective Zugriffsverwaltung aus.
3. Wählen Sie unter Meine Mitgliedskonten das Kontrollkästchen für jedes Mitgliedskonto aus, das Sie aktivieren möchten.

Sie können nur Mitgliedskonten aktivieren, die den Status Nicht aktiviert haben.

4. Wählen Sie Konten aktivieren.

Detective bestimmt, ob das Mitgliedskonto aktiviert werden kann. Wenn das Mitgliedskonto aktiviert werden kann, ändert sich der Status in Aktiviert.

Aktivierung eines Mitgliedskontos, das nicht aktiviert ist (Detective API, AWS CLI)

Sie können einen API-Aufruf oder den verwenden AWS Command Line Interface , um ein einzelnes Mitgliedskonto zu aktivieren, das nicht aktiviert ist. Verwenden Sie die Operation [ListGraphs](#), um den ARN Ihres Verhaltensdiagramms zur Verwendung in der Anfrage abzurufen.

So aktivieren Sie ein Mitgliedskonto, das nicht aktiviert ist

- Detective API: Verwenden Sie die API-Operation [StartMonitoringMember](#). Sie müssen den Verhaltensdiagramm-ARN angeben. Verwenden Sie die Konto-ID, um das AWS Mitgliedskonto zu identifizieren.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl [start-monitoring-member](#) aus:

```
start-monitoring-member --graph-arn <behavior graph ARN> --account-id <AWS account ID>
```

Beispielsweise:

```
start-monitoring-member --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 --account-id 444455556666
```

Mitgliedskonten aus einem Verhaltensdiagramm entfernen

Das Administratorkonto kann Mitgliedskonten jederzeit aus einem Verhaltensdiagramm entfernen.

Detective entfernt automatisch Mitgliedskonten AWS, die in den Regionen AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) gekündigt wurden.

Wenn ein Konto eines eingeladenen Mitglieds aus einem Verhaltensdiagramm entfernt wird, passiert Folgendes.

- Das Mitgliedskonto wird aus Meine Mitgliedskonten entfernt.
- Amazon Detective beendet die Aufnahme von Daten aus dem entfernten Konto.

Detective entfernt keine vorhandenen Daten aus dem Verhaltensdiagramm, das Daten über Mitgliedskonten hinweg aggregiert.

Mitgliedskonten aus einem Verhaltensdiagramm entfernen (Konsole)

Sie können das verwenden AWS Management Console , um Konten eingeladener Mitglieder aus Ihrem Verhaltensdiagramm zu entfernen.

So entfernen Sie Mitgliedskonten (Konsole)

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich von Detective Zugriffsverwaltung aus.
3. Aktivieren Sie in der Kontoliste das Kontrollkästchen für jedes Mitgliedskonto, das Sie entfernen möchten.

Sie können Ihr eigenes Konto nicht aus der Liste entfernen.

4. Wählen Sie Aktionen. Wählen Sie dann Konten deaktivieren.

Konten eingeladener Mitglieder aus einem Verhaltensdiagramm entfernen (Detective API, AWS CLI)

Sie können die Detective API oder die verwenden AWS Command Line Interface , um Konten eingeladener Mitglieder aus Ihrem Verhaltensdiagramm zu entfernen. Verwenden Sie die Operation [ListGraphs](#), um den ARN Ihres Verhaltensdiagramms zur Verwendung in der Anfrage abzurufen.

Um Konten eingeladener Mitglieder aus Ihrem Verhaltensdiagramm zu entfernen (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [DeleteMembers](#). Geben Sie den Diagramm-ARN und die Liste der Kontokennungen für die Mitgliedskonten an, die entfernt werden sollen.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl [delete-members](#) aus.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior graph ARN>
```

Beispiel:

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Eine Liste eingeladener Mitgliedskonten aus allen Regionen entfernen (Python-Skript aktiviert GitHub)

Detective bietet ein Open-Source-Skript in GitHub. Sie können dieses Skript verwenden, um eine bestimmte Liste von Mitgliedskonten aus den Verhaltensdiagrammen eines Administratorkontos in einer bestimmten Liste von Regionen zu entfernen.

Informationen zur Konfiguration und Verwendung der GitHub Skripts finden Sie unter [the section called “Amazon Detective Python-Skripte”](#).

Für Mitgliedskonten: Einladungen und Mitgliedschaften im Verhaltensdiagramm verwalten

Amazon Detective berechnet jedem Mitgliedskonto die aufgenommenen Daten für jedes Verhaltensdiagramm, zu dem es beiträgt.

Auf der Kontoverwaltungsseite können Mitgliedskonten die Administratorkonten anhand der Verhaltensdiagramme einsehen, in denen sie Mitglied sind.

Mitgliedskonten, die zu einem Verhaltensdiagramm eingeladen wurden, können ihre Einladungen einsehen und darauf antworten. Sie können ihr Konto auch aus dem Verhaltensdiagramm entfernen.

Im Verhaltensdiagramm der Organisation haben Organisationskonten keinen Einfluss darauf, ob es sich bei ihrem Konto um ein Mitgliedskonto handelt. Das Detective-Administratorkonto wählt die Organisationskonten aus, die als Mitgliedskonten aktiviert oder deaktiviert werden sollen.

Inhalt

- [Erforderliche IAM-Richtlinie für ein Mitgliedskonto](#)
- [Ihre Liste mit Einladungen im Verhaltensdiagramm anzeigen](#)
- [Auf eine Einladung zu einem Verhaltensdiagramm antworten](#)
- [Ihr Konto aus einem Verhaltensdiagramm entfernen](#)

Erforderliche IAM-Richtlinie für ein Mitgliedskonto

Bevor ein Mitgliedskonto Einladungen anzeigen und verwalten kann, muss die erforderliche IAM-Richtlinie seinem Hauptbenutzer zugewiesen werden. Der Prinzipal kann ein vorhandener Benutzer oder eine vorhandene Rolle sein, oder Sie können einen neuen Benutzer oder eine neue Rolle erstellen, die für Detective verwendet werden sollen.

Idealerweise fügt der IAM-Administrator dem Administratorkonto die erforderliche Richtlinie zu.

Die IAM-Richtlinie für Mitgliedskonten gewährt Zugriff auf Mitgliedskontoaktionen in Amazon Detective. Die E-Mail-Einladung, zu einem Verhaltensdiagramm beizutragen, enthält den Text dieser IAM-Richtlinie.

Um diese Richtlinie zu verwenden, *<behavior graph ARN>* ersetzen Sie durch den Diagramm-ARN.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:DisassociateMembership",
        "detective:RejectInvitation"
      ],
      "Resource": "<behavior graph ARN>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "detective:BatchGetMembershipDatasources",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations"
      ],
      "Resource": "*"
    }
  ]
}
```

Beachten Sie, dass Organisationskonten im Verhaltensdiagramm der Organisation keine Einladungen erhalten und dass ihr Konto nicht vom Organisationsverhaltensdiagramm getrennt werden kann. Wenn sie nicht zu anderen Verhaltensdiagrammen gehören, benötigen sie lediglich die ListInvitations-Genehmigung. ListInvitations ermöglicht es ihnen, das Administratorkonto für das Verhaltensdiagramm zu sehen. Die Berechtigungen zum Verwalten von Einladungen und zum Trennen von Mitgliedschaften gelten nur für Mitgliedschaften auf Einladung.

Ihre Liste mit Einladungen im Verhaltensdiagramm anzeigen

Von der Amazon Detective-Konsole, der Detective-API oder AWS Command Line Interface einem Mitgliedskonto aus können die Einladungen in einem Verhaltensdiagramm angezeigt werden.

Einladungen mit Verhaltensdiagramm anzeigen (Konsole)

Sie können Einladungen mit Verhaltensdiagrammen unter anzeigen AWS Management Console.

So zeigen Sie Einladungen im Verhaltensdiagramm an (Konsole)

1. Melden Sie sich bei der an AWS Management Console. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich von Detective Zugriffsverwaltung aus.

Auf der Seite Kontoverwaltung finden Sie unter Meine Administratorkonten Ihre offenen und akzeptierten Einladungen mit Verhaltensdiagrammen in der aktuellen Region. Für ein Organisationskonto enthält Meine Administratorkonten auch das Verhaltensdiagramm der Organisation.

Wenn sich Ihr Konto derzeit in der kostenlosen Testphase befindet, wird auf der Seite auch die Anzahl der Tage angezeigt, die noch in Ihrer kostenlosen Testversion verbleiben.

Die Liste enthält keine Einladungen, die Sie abgelehnt haben, Mitgliedschaften, die Sie gekündigt haben, oder Mitgliedschaften, die das Administratorkonto entfernt hat.

Jede Einladung enthält die Administratorkontonummer, das Datum, an dem die Einladung angenommen wurde, und den aktuellen Status der Einladung.

- Bei Einladungen, auf die Sie nicht geantwortet haben, lautet der Status Eingeladen.
- Für Einladungen, die Sie angenommen haben, lautet der Status entweder Aktiviert oder Nicht aktiviert.

Wenn der Status Aktiviert lautet, trägt Ihr Konto Daten zum Verhaltensdiagramm bei.

Wenn der Status Nicht aktiviert lautet, trägt Ihr Konto keine Daten zum Verhaltensdiagramm bei.

Ihr Kontostatus ist zunächst auf Nicht aktiviert gesetzt, während Detective prüft, ob Sie die GuardDuty Aktivierung aktiviert haben und wenn ja, ob Ihr Konto dazu führen würde, dass das Datenvolumen für das Verhaltensdiagramm das Detective-Kontingent überschreitet.

Wenn Ihr Konto nicht dazu führen würde, dass das Verhaltensdiagramm das Kontingent überschreitet, aktualisiert Detective Ihren Kontostatus auf Aktiviert. Andernfalls bleibt der Status Nicht aktiviert.

Wenn das Verhaltensdiagramm das Datenvolumen für Ihr Konto berücksichtigen kann, aktualisiert Detective es automatisch auf Aktiviert. Beispielsweise kann das Administratorkonto andere Mitgliedskonten entfernen, sodass Ihr Konto aktiviert werden kann. Das Administratorkonto kann Ihr Konto auch manuell aktivieren.

Einladungen in Verhaltensdiagrammen anzeigen (Detective API, AWS CLI)

Sie können Einladungen mit Verhaltensdiagrammen von der Detective API oder der AWS Command Line Interface auflisten.

So rufen Sie eine Liste offener und akzeptierter Einladungen zu Verhaltensdiagrammen ab (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [ListInvitations](#).
- AWS CLI: Führen Sie in der Befehlszeile den Befehl [list-invitations](#) aus.

```
aws detective list-invitations
```

Auf eine Einladung zu einem Verhaltensdiagramm antworten

Wenn Sie eine Einladung annehmen, wird Ihr Kontostatus zunächst auf Nicht aktiviert gesetzt, während Detective prüft, ob Ihr Konto dazu führen würde, dass das Datenvolumen für das Verhaltensdiagramm das Detective-Kontingent überschreitet. Damit Detective diese Prüfung durchführen kann, muss Amazon für Ihr Konto mindestens 48 Stunden lang GuardDuty aktiviert sein.

Wenn Ihr Konto nicht dazu führen würde, dass das Verhaltensdiagramm das Kontingent überschreitet, aktualisiert Detective Ihren Kontostatus auf Aktiviert. Ab diesem Zeitpunkt beginnt Detective damit, Daten aus Protokollen und Erkenntnissen aufzunehmen und in das Verhaltensdiagramm zu extrahieren. Ihr Konto wird für die Daten belastet.

Wenn das Hinzufügen Ihres Kontos dazu führen würde, dass das Datenvolumen für das Verhaltensdiagramm das Detective-Kontingent überschreitet, oder wenn Sie es nicht GuardDuty aktiviert haben, bleibt der Status Nicht aktiviert. In diesem Fall aktiviert Detective Ihr Konto automatisch, sofern Sie Ihr Konto nicht entfernen, sobald das Verhaltensdiagramm dies zulässt. Das Administratorkonto kann Ihr Konto auch manuell aktivieren.

Wenn Sie die Einladung ablehnen, wird sie aus Ihrer Einladungsliste entfernt und Detective verwendet Ihre Kontodaten nicht im Verhaltensdiagramm.

Auf eine Einladung zu einem Verhaltensdiagramm antworten (Konsole)

Sie können den verwenden AWS Management Console , um auf die E-Mail-Einladung zu antworten, die einen Link zur Detective-Konsole enthält. Sie können nur auf eine Einladung antworten, die den Status Eingeladen hat.

So antworten Sie auf eine Einladung zu einem Verhaltensdiagramm (Konsole)

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich von Detective Zugriffsverwaltung aus.
3. Um die Einladung anzunehmen und Daten zum Verhaltensdiagramm beizutragen, wählen Sie unter Meine Administratorkonten die Option Einladung annehmen aus.

Um die Einladung abzulehnen und sie aus der Liste zu entfernen, wählen Sie Ablehnen.

Auf eine Einladung mit einem Verhaltensdiagramm antworten (Detective API, AWS CLI)

Sie können auf Einladungen zu Verhaltensdiagrammen von der Detective API oder der AWS Command Line Interface antworten.

Um eine Einladung zum Verhaltensdiagramm anzunehmen (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [AcceptInvitation](#). Sie müssen den Diagramm-ARN angeben.

- AWS CLI: Führen Sie in der Befehlszeile den Befehl [accept-invitation](#) aus.

```
aws detective accept-invitation --graph-arn <behavior graph ARN>
```

Beispiel:

```
aws detective accept-invitation --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Um eine Einladung zum Verhaltensdiagramm abzulehnen (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [RejectInvitation](#). Sie müssen den Diagramm-ARN angeben.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl [reject-invitation](#) aus.

```
aws detective reject-invitation --graph-arn <behavior graph ARN>
```

Beispiel:

```
aws detective reject-invitation --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Ihr Konto aus einem Verhaltensdiagramm entfernen

Nachdem Sie eine Einladung angenommen haben, können Sie Ihr Konto jederzeit aus einem Verhaltensdiagramm entfernen. Wenn Sie Ihr Konto aus einem Verhaltensdiagramm entfernen, beendet Amazon Detective die Aufnahme von Daten aus Ihrem Konto in das Verhaltensdiagramm. Bestehende Daten verbleiben im Verhaltensdiagramm.

Nur eingeladene Konten können ihr Konto aus einem Verhaltensdiagramm entfernen. Organisationskonten können ihr Konto nicht aus dem Verhaltensdiagramm der Organisation entfernen.

Ihr Konto aus einem Verhaltensdiagramm entfernen (Konsole)

Sie können das verwenden AWS Management Console , um Ihr Konto aus einem Verhaltensdiagramm zu entfernen.

So entfernen Sie Ihr Konto aus einem Verhaltensdiagramm (Konsole)

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich von Detective Zugriffsverwaltung aus.
3. Wählen Sie unter Meine Administratorkonten für das Verhaltensdiagramm, von dem Sie kündigen möchten, die Option Kündigen aus.

Ihr Konto aus einem Verhaltensdiagramm entfernen (Detective API, AWS CLI)

Sie können die Detective API oder die verwenden AWS Command Line Interface , um Ihr Konto aus einem Verhaltensdiagramm zu entfernen.

Um Ihr Konto aus einem Verhaltensdiagramm zu entfernen (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [DisassociateMembership](#). Sie müssen den Diagramm-ARN angeben.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl [disassociate-membership](#) aus.

```
aws detective disassociate-membership --graph-arn <behavior graph ARN>
```

Beispiel:

```
aws detective disassociate-membership --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Auswirkung von Kontoaktionen auf Verhaltensdiagramme

Diese Aktionen haben die folgenden Auswirkungen auf die Daten und den Zugriff von Amazon Detective.

Detective deaktiviert

Wenn ein Administratorkonto Detective deaktiviert, geschieht Folgendes:

- Das Verhaltensdiagramm wird entfernt.
- Detective beendet die Aufnahme von Daten aus dem Administratorkonto und den Mitgliedskonten für dieses Verhaltensdiagramm.

Das Mitgliedskonto wird aus dem Verhaltensdiagramm entfernt.

Wenn ein Mitgliedskonto aus einem Verhaltensdiagramm entfernt wird, hört Detective auf, Daten von diesem Konto aufzunehmen.

Bestehende Daten im Verhaltensdiagramm sind davon nicht betroffen.

Bei Konten mit Einladung wird das Konto aus der Liste Meine Mitgliedskonten entfernt.

Bei Organisationskonten im Verhaltensdiagramm der Organisation ändert sich der Kontostatus auf Kein Mitglied.

Das Mitgliedskonto verlässt die Organisation

Wenn ein Mitgliedskonto eine Organisation verlässt, geschieht Folgendes:

- Das Konto wird aus der Liste Meine Mitgliedskonten für das Verhaltensdiagramm der Organisation entfernt.
- Detective hört auf, Daten von diesem Konto aufzunehmen.

Bestehende Daten im Verhaltensdiagramm sind davon nicht betroffen.

AWS Konto gesperrt

Wenn ein Administratorkonto gesperrt wird AWS, verliert das Konto die Berechtigung, das Verhaltensdiagramm in Detective anzuzeigen. Detective hört auf, Daten in das Verhaltensdiagramm aufzunehmen.

Wenn ein Mitgliedskonto gesperrt wird AWS, hört Detective auf, Daten für dieses Konto zu erfassen.

Nach 90 Tagen wird das Konto entweder gekündigt oder reaktiviert. Wenn ein Administratorkonto reaktiviert wird, werden seine Detective-Berechtigungen wiederhergestellt. Detective nimmt die Aufnahme von Daten aus dem Konto wieder auf. Wenn ein Mitgliedskonto reaktiviert wird, nimmt Detective die Aufnahme von Daten aus dem Konto wieder auf.

AWS Konto geschlossen

Wenn ein AWS Konto geschlossen wird, reagiert Detective wie folgt auf die Schließung.

- Für ein Administratorkonto löscht Detective das Verhaltensdiagramm.
- Für ein Mitgliedskonto entfernt Detective das Konto aus dem Verhaltensdiagramm.

AWS bewahrt die Richtliniendaten für das Konto für einen Zeitraum von 90 Tagen ab dem Datum des Inkrafttretens der Schließung des Administratorkontos auf. Löscht am Ende des Zeitraums von 90 Tagen AWS dauerhaft alle Versicherungsdaten für das Konto.

- Zum Aufbewahren von Erkenntnissen für mehr als 90 Tage können Sie die Richtlinien archivieren. Sie können auch eine benutzerdefinierte Aktion mit einer EventBridge Regel verwenden, um die Ergebnisse in einem S3-Bucket zu speichern.
- Solange die Richtliniendaten AWS beibehalten werden, wird das Konto beim erneuten Öffnen des geschlossenen Kontos AWS erneut als Dienstadministrator zugewiesen und die Dienstrichtliniendaten für das Konto wiederhergestellt.
- Weitere Informationen finden Sie unter [Schließen eines Kontos](#).

Important

Für Kunden in den Regionen: AWS GovCloud (US)

- Sichern Sie vor dem Schließen Ihres Kontos die Richtliniendaten und löschen Sie dann Kontoressourcen. Nach dem Schließen des Kontos haben Sie keinen Zugriff mehr darauf.

Verwenden der Amazon Detective Python-Skripte zur Verwaltung von Konten

Amazon Detective stellt eine Reihe von Open-Source-Python-Skripten im GitHub Repository [amazon-detective-multiaccount-scripts](#) bereit. Die Skripte benötigen Python 3.

Sie können diese nutzen, um die folgenden Aufgaben durchzuführen:

- Aktivieren Sie Detective für ein regionsübergreifendes Administratorkonto.

Wenn Sie Detective aktivieren, können Sie dem Verhaltensdiagramm Tag-Werte zuweisen.

- Fügen Sie Mitgliedskonten zu den Verhaltensdiagrammen eines Administratorkontos in allen Regionen hinzu.

- Senden Sie optional Einladungs-E-Mails an die Mitgliedskonten. Sie können die Anfrage auch so konfigurieren, dass keine Einladungs-E-Mails gesendet werden.
- Entfernen Sie Mitgliedskonten aus den regionsübergreifenden Verhaltensdiagrammen eines Administratorkontos.
- Deaktivieren Sie Detective für ein Administratorkonto in allen Regionen. Wenn ein Administratorkonto Detective deaktiviert, wird das Verhaltensdiagramm des Administratorkontos in jeder Region deaktiviert.

Überblick über das Skript **enableDetective.py**

Das `enableDetective.py`-Skript führt folgende Aktionen aus:

1. Aktiviert Detective für ein Administratorkonto in jeder angegebenen Region, falls für das Administratorkonto Detective in dieser Region noch nicht aktiviert ist.

Wenn Sie das Skript verwenden, um Detective zu aktivieren, können Sie dem Verhaltensdiagramm Tag-Werte zuweisen.

2. Sendet optional Einladungen vom Administratorkonto an die angegebenen Mitgliedskonten für jedes Verhaltensdiagramm.

Die Einladungs-E-Mail-Nachrichten verwenden den Standardnachrichteninhalt und können nicht angepasst werden.

Sie können die Anfrage auch so konfigurieren, dass keine Einladungs-E-Mails gesendet werden.

3. Nimmt die Einladungen für die Mitgliedskonten automatisch an.

Da das Skript die Einladungen automatisch annimmt, können Mitgliedskonten diese Nachrichten ignorieren.

Wir empfehlen, sich direkt an die Mitgliedskonten zu wenden, um sie darüber zu informieren, dass die Einladungen automatisch angenommen werden.

Überblick über das Skript **disableDetective.py**

Das `disableDetective.py`-Skript löscht die angegebenen Mitgliedskonten aus den Verhaltensdiagrammen des Administratorkontos in den angegebenen Regionen.

Es bietet auch eine Option zum Deaktivieren von Detective für das Administratorkonto in den angegebenen Regionen.

Erforderliche Berechtigungen für die Skripts

Die Skripts erfordern eine bereits bestehende AWS Rolle im Administratorkonto und in allen Mitgliedskonten, die Sie hinzufügen oder entfernen.

Note

Der Rollenname muss in allen Konten identisch sein.

In der IAM-Richtlinie [wird empfohlen](#), Rollen mit dem geringsten Geltungsbereich zu verwenden. Um den Arbeitsablauf des Skripts zum [Erstellen eines Diagramms](#), zum [Erstellen von Elementen](#) und zum [Hinzufügen von Elementen zum Diagramm](#) auszuführen, sind folgende Berechtigungen erforderlich:

- Detektiv: CreateGraph
- Detektiv: CreateMembers
- Detektiv: DeleteGraph
- Detektiv: DeleteMembers
- Detektiv: ListGraphs
- Detektiv: ListMembers
- Detektiv: AcceptInvitation

Vertrauensbeziehung der Rolle

Das Rollenvertrauensverhältnis muss es Ihrer Instance oder Ihren lokalen Anmeldeinformationen ermöglichen, die Rolle zu übernehmen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
```

```
    "AWS": "arn:aws:iam::<ACCOUNTID>:user/<USERNAME>"
  },
  "Action": "sts:AssumeRole"
}
]
```

Wenn Sie nicht über eine gemeinsame Rolle verfügen, die die erforderlichen Berechtigungen umfasst, müssen Sie in jedem Mitgliedskonto eine Rolle mit mindestens diesen Berechtigungen erstellen. Sie müssen die Rolle auch im Administratorkonto erstellen.

Wenn Sie die Rolle erstellen, sollten Sie unbedingt wie folgt vorgehen:

- Verwenden Sie in jedem Konto denselben Rollennamen.
- Fügen Sie die oben genannten erforderlichen Berechtigungen hinzu (empfohlen) oder wählen Sie die [AmazonDetectiveFullAccess](#) verwaltete Richtlinie aus.
- Fügen Sie wie oben beschrieben einen Block für Rollenvertrauensbeziehungen hinzu.

Um diesen Prozess zu automatisieren, können Sie die `EnableDetective.yaml` AWS CloudFormation Vorlage verwenden. Da die Vorlage nur globale Ressourcen erstellt, kann sie in jeder Region ausgeführt werden.

Einrichtung der Ausführungsumgebung für die Python-Skripte

Sie können die Skripts entweder von einer EC2-Instance oder von einem lokalen Computer aus ausführen.

Starten und konfigurieren einer EC2-Instance

Eine Möglichkeit, die Skripts auszuführen, besteht darin, sie von einer EC2-Instance aus auszuführen.

Starten und konfigurieren einer EC2-Instance

1. Starten einer EC2-Instance in Ihrem Administratorkonto. Einzelheiten zum Starten einer EC2-Instance finden Sie unter [Erste Schritte mit Amazon EC2 EC2-Linux-Instances](#) im Amazon EC2 EC2-Benutzerhandbuch.
2. Fügen Sie der Instance eine IAM-Rolle mit den erforderlichen Berechtigungen hinzu, damit die Instance `AssumeRole` innerhalb des Administratorkontos Aufrufe tätigen kann.

Wenn Sie die `EnableDetective.yaml` AWS CloudFormation Vorlage verwendet haben, wurde eine Instance-Rolle mit einem Profil namens `EnableDetective` erstellt.

Andernfalls finden Sie Informationen zum Erstellen einer Instance-Rolle im Blogbeitrag [Einfache Ersetzung oder Anfügen einer IAM-Rolle an eine bestehende EC2-Instance mithilfe der EC2-Konsole](#).

3. Installieren der erforderlichen Software:

- APT: `sudo apt-get -y install python3-pip python3 git`
- RPM: `sudo yum -y install python3-pip python3 git`
- Boto (Mindestversion 1.15): `sudo pip install boto3`

4. Klonen Sie das Repository auf die EC2-Instanz.

```
git clone https://github.com/aws-samples/amazon-detective-multiaccount-scripts.git
```

Konfiguration eines lokalen Computers zur Ausführung der Skripts

Sie können die Skripts auch von Ihrem lokalen Computer aus ausführen.

So konfigurieren Sie einen lokalen Computer für die Ausführung der Skripts

1. Stellen Sie sicher, dass Sie auf Ihrem lokalen Computer Anmeldeinformationen für Ihr Administratorkonto eingerichtet haben, mit denen Sie `AssumeRole` aufrufen können.
2. Installieren der erforderlichen Software:
 - Python 3
 - Boto (Mindestversion 1.15)
 - GitHub Skripte

Plattform	Anweisungen zur Einrichtung
Windows	<ol style="list-style-type: none"> 1. Installieren Sie Python 3 (https://www.python.org/downloads/windows/). 2. Öffnen Sie eine Befehlszeile.

Plattform	Anweisungen zur Einrichtung
	<ol style="list-style-type: none"> Um Boto zu installieren, führen Sie folgenden Befehl aus: <code>pip install boto3</code> Laden Sie den Quellcode des Skripts von GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts) herunter.
Mac	<ol style="list-style-type: none"> Installieren Sie Python 3 (https://www.python.org/downloads/mac-osx/). Öffnen Sie eine Befehlszeile. Um Boto zu installieren, führen Sie folgenden Befehl aus: <code>pip install boto3</code> Laden Sie den Quellcode des Skripts von GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts) herunter.
Linux	<ol style="list-style-type: none"> Führen Sie einen der folgenden Schritte aus, um Python 3 zu installieren: <ul style="list-style-type: none"> <code>sudo apt-get -y install python3-pip python3 git</code> <code>sudo yum install git python</code> Um Boto zu installieren, führen Sie folgenden Befehl aus: <code>sudo pip install boto3</code> Klonen Sie den Skriptquellcode von https://github.com/aws-samples/amazon-detective-multiaccount-scripts.

Erstellen einer `.csv`-Liste von Mitgliedskonten, die hinzugefügt oder entfernt werden sollen

Um die Mitgliedskonten zu identifizieren, die zu den Verhaltensdiagrammen hinzugefügt oder daraus entfernt werden sollen, stellen Sie eine `.csv`-Datei bereit, die die Liste der Konten enthält.

Führen Sie jedes Konto in einer separaten Zeile auf. Jeder Mitgliedskontoeintrag enthält die AWS Konto-ID und die Root-Benutzer-E-Mail-Adresse des Kontos.

Sehen Sie sich das folgende Beispiel an:

```
111122223333,srodriguez@example.com  
444455556666,rroe@example.com
```

Ausführen von **enableDetective.py**

Sie können das `enableDetective.py`-Skript von einer EC2-Instanz oder Ihrem lokalen Computer aus ausführen.

So führen Sie **enableDetective.py** aus

1. Kopieren Sie die `.csv`-Datei in das `amazon-detective-multiaccount-scripts`-Verzeichnis auf Ihrer EC2-Instanz oder Ihrem lokalen Computer.
2. Wechseln Sie in das `amazon-detective-multiaccount-scripts`-Verzeichnis.
3. Führen Sie das `enableDetective.py`-Skript aus.

```
enableDetective.py --master_account administratorAccountID --assume_role roleName  
--input_file inputFileName --tags tagValueList --enabled_regions regionList --  
disable_email
```

Ersetzen Sie bei der Ausführung des Skripts die folgenden Werte:

administratorAccountID

Die AWS Konto-ID für das Administratorkonto.

roleName

Der Name der AWS Rolle, die im Administratorkonto und in jedem Mitgliedskonto übernommen werden soll.

inputFileName

Der Name der `.csv`-Datei, die die Liste der Mitgliedskonten enthält, die zu den Verhaltensdiagrammen des Administratorkontos hinzugefügt werden sollen.

tagValueList

(Optional) Eine komma-getrennte Liste von Tag-Werten, die einem neuen Verhaltensdiagramm zugewiesen werden sollen.

Für jeden Tag-Wert lautet das Format *key=value*. Beispielsweise:

```
--tags Department=Finance,Geo=Americas
```

regionList

(Optional) Eine komma-getrennte Liste von Regionen, in denen die Mitgliedskonten dem Verhaltensdiagramm des Administratorkontos hinzugefügt werden sollen. Beispielsweise:

```
--enabled_regions us-east-1,us-east-2,us-west-2
```

Für das Administratorkonto ist Detective möglicherweise noch nicht in einer Region aktiviert. In diesem Fall aktiviert das Skript Detective und erstellt ein neues Verhaltensdiagramm für das Administratorkonto.

Wenn Sie keine Liste mit Regionen angeben, funktioniert das Skript in allen Regionen, die Detective unterstützt.

`--disable_email`

(Optional) Falls enthalten, sendet Detective keine Einladungs-E-Mails an die Mitgliedskonten.

Ausführen von **disableDetective.py**

Sie können das `disableDetective.py`-Skript von einer EC2-Instanz oder Ihrem lokalen Computer aus ausführen.

So führen Sie **disableDetective.py** aus

1. Kopieren Sie die `.csv`-Datei in das Verzeichnis `amazon-detective-multiaccount-scripts`.
2. Um die `.csv`-Datei zu verwenden, um die aufgelisteten Mitgliedskonten aus den Verhaltensdiagrammen des Administratorkontos in einer bestimmten Liste von Regionen zu löschen, führen Sie das `disableDetective.py`-Skript wie folgt aus:

```
disabledetective.py --master_account administratorAccountID --assume_role roleName  
--input_file inputFileName --disabled_regions regionList
```

3. Um Detective für das Administratorkonto in allen Regionen zu deaktivieren, führen Sie das `disableDetective.py`-Skript mit der `--delete-master`-Markierung aus.

```
disabledetective.py --master_account administratorAccountID --assume_role roleName  
--input_file inputFileName --disabled_regions regionList --delete_master
```

Ersetzen Sie bei der Ausführung des Skripts die folgenden Werte:

administratorAccountID

Die AWS Konto-ID für das Administratorkonto.

roleName

Der Name der AWS Rolle, die im Administratorkonto und in jedem Mitgliedskonto übernommen werden soll.

inputFileName

Der Name der .csv-Datei, die die Liste der Mitgliedskonten enthält, die aus den Verhaltensdiagrammen des Administratorkontos entfernt werden sollen.

Sie müssen eine .csv-Datei bereitstellen, auch wenn Sie Detective deaktivieren.

regionList

(Optional) Eine komma-getrennte Liste von Regionen, in denen einer der folgenden Schritte ausgeführt werden kann:

- Entfernen der Mitgliedskonten aus den Verhaltensdiagrammen des Administratorkontos.
- Wenn das `--delete-master`-Flag enthalten ist, Detective deaktivieren.

Beispielsweise:

```
--disabled_regions us-east-1,us-east-2,us-west-2
```

Wenn Sie keine Liste mit Regionen angeben, funktioniert das Skript in allen Regionen, die Detective unterstützt.

Integration mit Amazon Security Lake

Amazon Security Lake ist ein vollständig verwalteter Sicherheits-Data-Lake-Dienst. Sie können Security Lake verwenden, um Sicherheitsdaten aus AWS Umgebungen, SaaS-Anbietern, lokalen Quellen, Cloud-Quellen und Quellen von Drittanbietern automatisch in einem speziell entwickelten Data Lake zu zentralisieren, der in Ihrem Konto gespeichert wird. AWS Security Lake hilft Ihnen bei der Analyse von Sicherheitsdaten, sodass Sie sich ein umfassenderes Bild von der Sicherheitslage in Ihrem gesamten Unternehmen machen können. Mit Security Lake können Sie auch den Schutz Ihrer Workloads, Anwendungen und Daten verbessern.

Amazon Detective ist in Amazon Security Lake integriert, was bedeutet, dass Sie die von Security Lake gespeicherten Rohprotokolldaten abfragen und abrufen können.

Mithilfe dieser Integration können Sie Protokolle und Ereignisse aus den folgenden Quellen sammeln, die Security Lake nativ unterstützt. Detective unterstützt bis zu Quellversion 2 (OCSF 1.1.0).

- AWS CloudTrail Verwaltungsereignisse Version 1.0 und höher
- Amazon Virtual Private Cloud (Amazon VPC) Flow Logs Version 1.0 und höher
- Auditprotokoll von Amazon Elastic Kubernetes Service (Amazon EKS), Version 2.0. Um Amazon EKS-Audit-Logs als Quelle `ram:ListResources` zu verwenden, müssen Sie die IAM-Berechtigungen erweitern. Weitere Informationen finden [Sie unter Hinzufügen der erforderlichen IAM-Berechtigungen zu Ihrem Konto](#).

Einzelheiten darüber, wie Security Lake Protokolle und Ereignisse, die von nativ unterstützten AWS Diensten stammen, automatisch in das OCSF-Schema konvertiert, finden Sie im [Amazon Security Lake-Benutzerhandbuch](#).

Nachdem Sie Detective in Security Lake integriert haben, beginnt Detective mit dem Abrufen von Rohprotokollen aus Security Lake, die sich auf AWS CloudTrail Verwaltungsereignisse und Amazon VPC Flow Logs beziehen. Weitere Informationen finden Sie unter [Abfragen von Rohprotokollen](#).

Führen Sie die folgenden Schritte aus, um Detective in Security Lake zu integrieren:

1. [Bevor Sie beginnen](#)

Verwenden Sie ein Organizations-Verwaltungskonto, um einen delegierten Security Lake-Administrator für Ihre Organisation festzulegen. Stellen Sie sicher, dass Security Lake aktiviert

ist, und stellen Sie sicher, dass Security Lake Protokolle und Ereignisse von AWS CloudTrail Verwaltungsereignissen und Amazon Virtual Private Cloud (Amazon VPC) Flow Logs sammelt.

In Übereinstimmung mit der Security Reference Architecture empfiehlt Detective, ein Log Archive-Konto zu verwenden und von der Verwendung eines Security Tooling-Kontos für die Security Lake-Bereitstellung abzusehen.

2. [Erstellen eines Security Lake-Abonnenten](#)

Um Protokolle und Ereignisse von Amazon Security Lake nutzen zu können, müssen Sie Security-Lake-Abonnent sein. Gehen Sie wie folgt vor, um einem Detective-Kontoadministrator Abfragezugriff zu gewähren.

3. Fügen Sie Ihrer IAM-Identität die erforderlichen AWS Identity and Access Management (IAM-) Berechtigungen hinzu.

- Fügen Sie diese Berechtigungen hinzu, um die Detective-Integration mit Security Lake zu erstellen:
 - Fügen Sie diese AWS Identitäts- und Zugriffsverwaltungsberechtigungen (IAM) Ihrer IAM-Identität hinzu. Einzelheiten finden Sie im Abschnitt [Hinzufügen der erforderlichen IAM-Berechtigungen zu Ihrem Konto](#).
 - Fügen Sie diese IAM-Richtlinie dem IAM-Prinzipal hinzu, den Sie zur Weitergabe der AWS CloudFormation Servicerolle verwenden möchten. Weitere Informationen finden Sie im Abschnitt [Hinzufügen von Berechtigungen zu Ihrem IAM-Prinzipal](#).
 - Wenn Sie Detective bereits in Security Lake integriert haben, fügen Sie diese (IAM-) Berechtigungen Ihrer IAM-Identität hinzu, um die Integration zu verwenden. Einzelheiten finden Sie im Abschnitt [Hinzufügen der erforderlichen IAM-Berechtigungen zu Ihrem Konto](#).

4. [Annehmen der Resource Share ARN-Einladung und aktivieren der Integration](#)

Verwenden Sie die AWS CloudFormation Vorlage, um die Parameter einzurichten, die für die Erstellung und Verwaltung des Abfragezugriffs für Security Lake-Abonnenten erforderlich sind. Die detaillierten Schritte zum Erstellen eines Stacks finden Sie unter [Erstellen eines Stacks mithilfe der AWS CloudFormation Vorlage](#). Wenn Sie mit der Erstellung des Stacks fertig sind, aktivieren Sie die Integration.

Eine Demonstration der Integration von Amazon Detective mit Amazon Security Lake mithilfe der Detective-Konsole finden Sie im folgenden Video: [Amazon Detective-Integration mit Amazon Security Lake — Einrichtung](#) -->

Bevor Sie beginnen

Security Lake lässt sich integrieren AWS Organizations , um die Protokollerfassung für mehrere Konten in einer Organisation zu verwalten. Um Security Lake für eine Organisation verwenden zu können, muss Ihr AWS Organizations Verwaltungskonto zunächst einen delegierten Security Lake-Administrator für Ihr Unternehmen bestimmen. Der delegierte Security Lake-Administrator muss dann Security Lake aktivieren und die Protokoll- und Ereigniserfassung für Mitgliedskonten in der Organisation aktivieren.

Bevor Sie Security Lake mit Detective integrieren, stellen Sie sicher, dass Security Lake für das Security Lake-Administratorkonto aktiviert ist. Die detaillierten Schritte zur Aktivierung von Security Lake finden Sie unter [Erste Schritte](#) im Amazon-Security-Lake-Benutzerhandbuch.

Stellen Sie außerdem sicher, dass Security Lake Protokolle und Ereignisse von AWS CloudTrail Verwaltungsereignissen und Amazon Virtual Private Cloud (Amazon VPC) Flow Logs sammelt. Weitere Informationen zur Protokollerfassung in Security Lake finden Sie unter [Sammeln von Daten aus AWS Services](#) im Amazon Security Lake-Benutzerhandbuch.

Schritt 1: Erstellen eines Security Lake-Abonnenten

Um Protokolle und Ereignisse von Amazon Security Lake nutzen zu können, müssen Sie Security-Lake-Abonnent sein. Ein Abonnent kann die von Security Lake gesammelten Daten abfragen und darauf zugreifen. Ein Abonnent mit Abfragezugriff kann mithilfe von Diensten wie Amazon Athena AWS Lake Formation Tabellen direkt in einem Amazon Simple Storage Service (Amazon S3) -Bucket abfragen. Um Abonnent zu werden, muss Ihnen der Security Lake-Administrator Abonnentenzugriff gewähren, mit dem Sie den Data Lake abfragen können. Informationen dazu, wie der Administrator dabei vorgeht, finden Sie unter [Einen Abonnenten mit Abfragezugriff erstellen](#) im Amazon-Security-Lake-Benutzerhandbuch.

Gehen Sie wie folgt vor, um einem Detective-Kontoadministrator Abfragezugriff zu gewähren.

So erstellen Sie einen Detective-Abonnenten in Security Lake

1. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich Integrationen aus.
3. Notieren Sie sich im Abonnentenbereich von Security Lake die Werte Konto-ID und Externe ID.

Bitten Sie den Security Lake-Administrator, diese IDs für folgende Zwecke zu verwenden:

- So erstellen Sie einen Detective-Abonnenten für Sie in Security Lake.
- So konfigurieren Sie den Abonnenten für den Abfragezugriff.
- Wählen Sie Lake Formation als Datenzugriffsmethode in der Security-Lake-Konsole, um sicherzustellen, dass der Security-Lake-Abfrage-Abonnent mit Lake-Formation-Berechtigungen erstellt wurde.

Wenn der Security-Lake-Administrator einen Abonnenten für Sie erstellt, generiert Security Lake einen Amazon Resource Share ARN für Sie. Bitten Sie den Administrator, Ihnen diesen ARN zu senden.

4. Geben Sie den Resource Share ARN, der vom Security Lake-Administrator bereitgestellt wird, im Security Lake-Abonnentenbereich ein.
5. Nachdem Sie den Resource Share ARN vom Security Lake Administrator erhalten haben, geben Sie den ARN in das Feld Resource Share ARN im Security Lake-Abonnentenbereich ein.

Schritt 2: Fügen Sie die erforderlichen IAM-Berechtigungen zu Ihrem Konto hinzu

Um die Detective-Integration mit Security Lake zu aktivieren, müssen Sie Ihrer IAM-Identität die folgende AWS Identity and Access Management (IAM-) Berechtigungsrichtlinie hinzufügen.

Fügen Sie der Rolle die folgende Inline-Richtlinien an. Ersetzen Sie `athena-results-bucket` durch Ihren Amazon-S3-Bucket-Namen, wenn Sie Ihren eigenen Amazon-S3-Bucket zum Speichern der Athena-Abfrageergebnisse verwenden möchten. Wenn Sie möchten, dass Detective automatisch einen Amazon-S3-Bucket zum Speichern des Athena-Abfrageergebnisses generiert, entfernen Sie den gesamten `S3ObjectPermissions-Bucket` aus der IAM-Richtlinie.

Wenn Sie nicht über die erforderlichen Berechtigungen verfügen, um diese Richtlinie an Ihre IAM-Identität anzuhängen, wenden Sie sich an Ihren Administrator. AWS Wenn Sie über die erforderlichen Berechtigungen verfügen, aber ein Problem auftritt, finden Sie weitere Informationen unter [Behebung allgemeiner IAM-Probleme](#) im IAM-Benutzerhandbuch.

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

```

    "Action": [
      "s3:GetBucketLocation",
      "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
  },
  {
    "Sid": "S3ObjectPermissions",
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::<athena-results-bucket>",
      "arn:aws:s3:::<athena-results-bucket>/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "glue:GetDatabases",
      "glue:GetPartitions",
      "glue:GetTable",
      "glue:GetTables"
    ],
    "Resource": [
      "arn:aws:glue:*:<ACCOUNT ID>:database/amazon_security_lake*",
      "arn:aws:glue:*:<ACCOUNT ID>:table/amazon_security_lake*/
amazon_security_lake*",
      "arn:aws:glue:*:<ACCOUNT ID>:catalog"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "athena:BatchGetQueryExecution",
      "athena:GetQueryExecution",
      "athena:GetQueryResults",
      "athena:GetQueryRuntimeStatistics",
      "athena:GetWorkGroup",
      "athena:ListQueryExecutions",
      "athena:StartQueryExecution",
      "athena:StopQueryExecution",

```

```

    "lakeformation:GetDataAccess",
    "ram:ListResources"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "ssm:GetParametersByPath"
  ],
  "Resource": [
    "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/ResourceShareArn",
    "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/S3Bucket",
    "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/TableNames",
    "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/DatabaseName",
    "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/StackId"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "cloudformation:GetTemplateSummary",
    "iam:ListRoles"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "organizations:ServicePrincipal": [
        "securitylake.amazonaws.com"
      ]
    }
  }
}
]
}

```

Schritt 3: Annahme der Resource Share ARN-Einladung und Aktivieren der Integration

Um auf Rohdatenprotokolle von Security Lake zuzugreifen, müssen Sie eine Resource Share-Einladung von dem Security Lake-Konto annehmen, das vom Security Lake-Administrator erstellt wurde. Sie benötigen außerdem AWS Lake Formation -Berechtigungen, um die kontenübergreifende gemeinsame Nutzung von Tabellen einzurichten. Darüber hinaus müssen Sie einen Amazon Simple Storage Service (Amazon S3)-Bucket erstellen, der rohe Abfrageprotokolle empfangen kann.

In diesem nächsten Schritt verwenden Sie eine AWS CloudFormation Vorlage, um einen Stack zu erstellen für: Annahme der Resource Share ARN-Einladung, Erstellung erforderlicher AWS-Glue-Crawler Ressourcen und Erteilung von AWS Lake Formation Administratorberechtigungen.

Um einen AWS CloudFormation Stapel zu erstellen

1. Erstellen Sie mithilfe der CloudFormation Vorlage einen neuen CloudFormation Stapel. Weitere Details finden Sie unter [Erstellen eines Stacks mithilfe der AWS CloudFormation -Vorlage](#).
2. Wenn Sie mit der Erstellung des Stacks fertig sind, wählen Sie Integration aktivieren aus.

Erstellen eines Stacks mithilfe der AWS CloudFormation -Vorlage

Detective stellt eine AWS CloudFormation Vorlage bereit, mit der Sie die Parameter einrichten können, die für die Erstellung und Verwaltung des Abfragezugriffs für Security Lake-Abonnenten erforderlich sind.

Schritt 1: Erstellen Sie eine AWS CloudFormation Servicerolle

Sie müssen eine AWS CloudFormation Servicerolle erstellen, um mithilfe der AWS CloudFormation Vorlage einen Stack zu erstellen. Wenn Sie nicht über die erforderlichen Berechtigungen zum Erstellen einer Servicerolle verfügen, wenden Sie sich an den Administrator des Detective-Administratorkontos. Weitere Informationen zur AWS CloudFormation -Servicerolle finden Sie unter [AWS CloudFormation -Servicerolle](#).

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter <https://console.aws.amazon.com/iam/>.
2. Klicken Sie im Navigationsbereich der IAM-Konsole auf Rollen, und wählen Sie dann Rolle erstellen.

3. Wählen Sie für Select trusted entity (Vertrauenswürdige Entität auswählen) die Option AWS - Dienst.
4. Wählen Sie AWS CloudFormation. Wählen Sie anschließend Weiter.
5. Geben Sie einen Namen für die Rolle ein. z. B. CFN-DetectiveSecurityLakeIntegration.
6. Fügen Sie der Rolle die folgende Inline-Richtlinien an. Ersetzen Sie es <Account ID> durch Ihre AWS Konto-ID.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CloudFormationPermission",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateChangeSet"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:aws:transform/*"
      ]
    },
    {
      "Sid": "IamPermissions",
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:PutRolePolicy",
        "iam>DeleteRolePolicy",
        "iam>CreatePolicy",
        "iam>DeletePolicy",
        "iam:PassRole",
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource": [
        "arn:aws:iam::<ACCOUNT ID>:role/*",
        "arn:aws:iam::<ACCOUNT ID>:policy/*"
      ]
    }
  ]
}
```

```
    },
    {
      "Sid": "S3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3>DeleteBucket*",
        "s3:PutBucket*",
        "s3:GetBucket*",
        "s3:GetObject",
        "s3:PutEncryptionConfiguration",
        "s3:GetEncryptionConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid": "LambdaPermissions",
      "Effect": "Allow",
      "Action": [
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:GetFunction",
        "lambda:TagResource",
        "lambda:InvokeFunction"
      ],
      "Resource": [
        "arn:aws:lambda:*:<ACCOUNT ID>:function:*"
      ]
    },
    {
      "Sid": "CloudwatchPermissions",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs>DeleteLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
    },
    {
      "Sid": "KmsPermission",
      "Effect": "Allow",
```

```

        "Action": [
            "kms:Decrypt"
        ],
        "Resource": "arn:aws:kms:*:<ACCOUNT ID>:key/*"
    }
}

```

Schritt 2: Fügen Sie Berechtigungen zu Ihrem IAM-Prinzipal hinzu.

Sie benötigen die folgenden Berechtigungen, um einen Stack mithilfe der CloudFormation Servicerolle zu erstellen, die Sie im vorherigen Schritt erstellt haben. Fügen Sie dem IAM-Prinzipal, den Sie zur Weitergabe der CloudFormation Servicerolle verwenden möchten, die folgende IAM-Richtlinie hinzu. Gehen Sie dabei davon aus, dass dieser IAM-Prinzipal den Stack erstellt. Wenn Sie nicht über die erforderlichen Berechtigungen zum Hinzufügen der IAM-Richtlinie verfügen, wenden Sie sich an den Administrator des Detective-Administratorkontos.

Note

In der folgenden Richtlinie bezieht sich die in dieser Richtlinie verwendete CFN-DetectiveSecurityLakeIntegration auf die Rolle, die Sie im vorherigen Schritt für die Creating an AWS CloudFormation-Servicerolle erstellt haben. Ändern Sie sie in den Rollennamen, den Sie im vorherigen Schritt eingegeben haben, falls es sich um einen anderen Namen handelt.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PassRole",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::<ACCOUNT ID>:role/CFN-DetectiveSecurityLakeIntegration"
    },
  ],
}

```

```

    {
      "Sid": "RestrictCloudFormationAccess",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*",
      "Condition": {
        "StringEquals": {
          "cloudformation:RoleArn": [
            "arn:aws:iam:*:<ACCOUNT ID>:role/CFN-
DetectiveSecurityLakeIntegration"
          ]
        }
      }
    },
    {
      "Sid": "CloudformationDescribeStack",
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetStackPolicy"
      ],
      "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*"
    },
    {
      "Sid": "CloudformationListStacks",
      "Effect": "Allow",
      "Action": [
        "cloudformation:ListStacks"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatchPermissions",
      "Effect": "Allow",
      "Action": [
        "logs:GetLogEvents"
      ],
      "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
    }
  }

```

```
]
}
```

Schritt 3: Geben Sie benutzerdefinierte Werte in der Konsole an AWS CloudFormation

1. Gehe von Detective zur AWS CloudFormation Konsole.
2. (Optional) Geben Sie einen Stack-Namen ein. Der Stackname wird automatisch ausgefüllt. Sie können den Stack-Namen in einen Namen ändern, der nicht mit den vorhandenen Stack-Namen kollidiert.
3. Legen Sie die folgenden Parameter fest.
 - AthenaResultsBucket— Wenn Sie keine Werte eingeben, generiert diese Vorlage einen Amazon S3 S3-Bucket. Wenn Sie Ihren eigenen Bucket verwenden möchten, geben Sie einen Bucket-Namen ein, um die Athena-Abfrageergebnisse zu speichern. Wenn Sie Ihren eigenen Bucket verwenden, stellen Sie sicher, dass sich der Bucket in derselben Region wie der Resource Share ARN befindet. Wenn Sie Ihren eigenen Bucket verwenden, stellen Sie sicher, dass die gewählte LakeFormationPrincipals über die Rechte verfügt, Objekte in den Bucket zu schreiben und Objekte aus dem Bucket zu lesen. Weitere Informationen über Bucket-Berechtigungen finden Sie unter [Abfragen und aktuelle Abfragen](#) im Benutzerhandbuch zu Amazon Athena.
 - DTRegion – Dieses Feld ist vorausgefüllt. Ändern Sie die Werte in diesem Feld nicht.
 - LakeFormationPrincipals— Geben Sie den ARN der IAM-Prinzipale (z. B. den ARN der IAM-Rolle) ein, denen Sie Zugriff für die Nutzung der Security Lake-Integration gewähren möchten, getrennt durch Kommas. Dies könnten Ihre Sicherheitsanalysten und Sicherheitsingenieure sein, die Detective verwenden.

Sie können nur die IAM-Prinzipale verwenden, denen Sie zuvor in Schritt [Step 2: Add the required IAM permissions to your account] die IAM-Berechtigungen zugewiesen haben.

- ResourceShareARN — Dieses Feld ist vorausgefüllt. Ändern Sie die Werte in diesem Feld nicht.
4. Berechtigungen

IAM-Rolle: Wählen Sie die Rolle aus, die Sie im Schritt `Creating an AWS CloudFormation Service Role` erstellt haben. Optional können Sie das Feld leer lassen, wenn Ihre aktuelle IAM-Rolle über alle erforderlichen Berechtigungen für den `Creating an AWS CloudFormation Service Role`-Schritt verfügt.

5. Überprüfen und aktivieren Sie alle Kontrollkästchen Ich bestätige und klicken Sie dann auf die Schaltfläche Stack erstellen. Weitere Informationen finden Sie in den folgenden IAM-Ressourcen, die erstellt werden.

```

* ResourceShareAcceptorCustomResourceFunction
  - ResourceShareAcceptorLambdaRole
  - ResourceShareAcceptorLogsAccessPolicy
* SsmParametersCustomResourceFunction
  - SsmParametersLambdaRole
  - SsmParametersLogsAccessPolicy
* GlueDatabaseCustomResourceFunction
  - GlueDatabaseLambdaRole
  - GlueDatabaseLogsAccessPolicy
* GlueTablesCustomResourceFunction
  - GlueTablesLambdaRole
  - GlueTablesLogsAccessPolicy

```

Schritt 4: Hinzufügen der Amazon-S3-Bucket-Richtlinie zu IAM-Prinzipalen in **LakeFormationPrincipals**

(Optional) Wenn Sie zulassen, dass diese Vorlage automatisch einen AthenaResultsBucket für Sie generiert, müssen Sie die folgende Richtlinie an die IAM-Prinzipale in LakeFormationPrincipals anhängen.

```

{
  "Sid": "S3ObjectPermissions",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::<athena-results-bucket>",
    "arn:aws:s3:::<athena-results-bucket>/*"
  ]
}

```

Durch den AthenaResultsBucket Namen athena-results-bucket ersetzen. Das AthenaResultsBucket kann auf der AWS CloudFormation Konsole gefunden werden:

1. Öffnen Sie die AWS CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation>.
2. Klicken Sie auf Ihren Stack.
3. Klicken Sie auf die Registerkarte Ressourcen.
4. Suchen Sie nach der logischen ID AthenaResultsBucket und kopieren Sie ihre physische ID.

Einen CloudFormation Stack löschen

Wenn Sie den vorhandenen Stack nicht löschen, schlägt die Erstellung eines neuen Stacks in derselben Region fehl. Sie können einen CloudFormation Stack mithilfe der CloudFormation Konsole oder der AWS CLI löschen.

Um den AWS CloudFormation Stack zu löschen (Konsole)

1. Öffnen Sie die AWS CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation>.
2. Wählen Sie auf der Seite Stacks in der CloudFormation Konsole den Stack aus, den Sie löschen möchten. Der Stack muss aktuell ausgeführt werden.
3. Wählen Sie im Stack-Detailbereich Delete (Löschen) aus.
4. Wählen Sie Delete stack (Stack löschen) aus, wenn Sie dazu aufgefordert werden.

Note

Der Stack-Löschvorgang kann nicht gestoppt werden, sobald die Stack-Löschung begonnen hat. Der Stack wird in den Status DELETE_IN_PROGRESS versetzt.

Nachdem die Löschung des Stapels abgeschlossen ist, befindet sich der Stack im Status DELETE_COMPLETE.

Behebung von Fehlern beim Löschen von Stacks

Wenn Sie `Failed to delete stack` nach dem Klicken auf die `Delete` Schaltfläche einen Berechtigungsfehler mit der Meldung sehen, ist Ihre IAM-Rolle nicht CloudFormation berechtigt, einen Stack zu löschen. Wenden Sie sich an Ihren Kontoadministrator, um den Stack zu löschen.

Um den CloudFormation Stack zu löschen (AWS CLI)

Geben Sie den folgenden Befehl in die AWS CLI-Schnittstelle ein:

```
aws cloudformation delete-stack --stack-name your-stack-name --role-arn
arn:aws:iam::<ACCOUNT ID>:role/CFN-DetectiveSecurityLakeIntegration
```

CFN-DetectiveSecurityLakeIntegration ist die Servicerolle, die Sie in diesem `Creating an AWS CloudFormation Service Role`-Schritt erstellt haben.

Ändern der Integrationskonfiguration

Wenn Sie einen der Parameter ändern möchten, die Sie zur Integration von Detective in Security Lake verwendet haben, können Sie ihn bearbeiten und dann die Integration erneut aktivieren. Sie können die AWS CloudFormation Vorlage bearbeiten, um diese Integration für die folgenden Szenarien wieder zu aktivieren:

- Zum Aktualisieren des Security-Lake-Abonnements können Sie entweder einen neuen Abonnenten erstellen oder der Security-Lake-Administrator kann die Datenquelle für das bestehende Abonnement aktualisieren.
- So legen Sie einen anderen Amazon-S3-Bucket zum Speichern der rohen Abfrageprotokolle fest.
- Um verschiedene Lake Formation-Prinzipale festzulegen.

Wenn Sie die Detective-Integration mit Security Lake erneut aktivieren, können Sie den Resource Share ARN bearbeiten und die IAM-Berechtigungen einsehen. Um die IAM-Berechtigungen zu bearbeiten, können Sie von Detective aus zur IAM-Konsole wechseln. Sie können auch die Werte bearbeiten, die Sie zuvor in die AWS CloudFormation Vorlage eingegeben haben. Sie müssen den vorhandenen CloudFormation Stack löschen und neu erstellen, um die Integration wieder zu aktivieren.

So reaktivieren Sie die Detective-Integration mit Security Lake

1. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich Integrationen aus.
3. Sie können die Integration mit einem der folgenden Schritte bearbeiten:
 - Wählen Sie im Bereich Security Lake die Option Bearbeiten aus.
 - Wählen Sie im Bereich Security Lake die Option Ansicht aus. Wählen Sie in der Ansichtsseite die Option Bearbeiten.

4. Geben Sie einen neuen Resource Share ARN ein, um auf die Datenquellen in einer Region zuzugreifen.
5. Sehen Sie sich die aktuellen IAM-Berechtigungen an, und rufen Sie die IAM-Konsole auf, wenn Sie die IAM-Berechtigungen bearbeiten möchten.
6. Bearbeiten Sie die Werte in der CloudFormation Vorlage.
 1. Löschen Sie zuerst den vorhandenen Stack, bevor Sie einen neuen Stack erstellen. Wenn Sie den vorhandenen Stack nicht löschen und versuchen, einen neuen Stack in derselben Region zu erstellen, schlägt Ihre Anfrage fehl. Weitere Details finden Sie unter [Einen CloudFormation Stack löschen](#).
 1. Erstellen Sie einen neuen CloudFormation Stapel. Weitere Details finden Sie unter [Erstellen eines Stacks mithilfe der AWS CloudFormation -Vorlage](#).
7. Wählen Sie Integration aktivieren aus.

Deaktivierung der Integration

Wenn Sie die Detective-Integration mit Security Lake deaktivieren, können Sie keine Protokoll- und Ereignisdaten mehr von Security Lake abfragen.

So deaktivieren Sie die Detective-Integration mit Security Lake

1. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich Integrationen aus.
3. Löschen Sie den vorhandenen Stack. Weitere Details finden Sie unter [Einen CloudFormation Stack löschen](#).
4. Wählen Sie im Bereich Security Lake-Integration deaktivieren die Option Deaktivieren aus.

Unterstützte AWS Regionen

Sie können Detective in Security Lake in den folgenden AWS Regionen integrieren.

Name der Region	Region	Endpoint	Protokoll
USA Ost (Ohio)	us-east-2	securitylake.us-east-2.amazonaws.com	HTTPS
USA Ost (Nord-Virginia)	us-east-1	securitylake.us-east-1.amazonaws.com	HTTPS
USA West (Nordkalifornien)	us-west-1	securitylake.us-west-1.amazonaws.com	HTTPS
USA West (Oregon)	us-west-2	securitylake.us-west-2.amazonaws.com	HTTPS
Asien-Pazifik (Mumbai)	ap-south-1	securitylake.ap-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Seoul)	ap-northeast-2	securitylake.ap-northeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Singapur)	ap-southeast-1	securitylake.ap-southeast-1.amazonaws.com	HTTPS
Asien-Pazifik (Sydney)	ap-southeast-2	securitylake.ap-southeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Tokio)	ap-northeast-1	securitylake.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Zentral)	ca-central-1	securitylake.ca-central-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	securitylake.eu-central-1.amazonaws.com	HTTPS
Europa (Irland)	eu-west-1	securitylake.eu-west-1.amazonaws.com	HTTPS

Name der Region	Region	Endpoint	Protokoll
Europa (London)	eu-west-2	securitylake.eu-west-2.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	securitylake.eu-west-3.amazonaws.com	HTTPS
Europa (Stockholm)	eu-north-1	securitylake.eu-north-1.amazonaws.com	HTTPS
Südamerika (São Paulo)	sa-east-1	securitylake.sa-east-1.amazonaws.com	HTTPS

Abfragen von Rohprotokollen in Detective

Nachdem Sie Detective in Security Lake integriert haben, beginnt Detective mit dem Abrufen von Rohprotokollen aus Security Lake, die sich auf AWS CloudTrail Verwaltungsereignisse und Amazon Virtual Private Cloud (Amazon VPC) Flow Logs beziehen.

Note

Für die Abfrage von Rohprotokollen in Detective fallen keine zusätzlichen Gebühren an. Nutzungsgebühren für andere AWS Services, einschließlich Amazon Athena, fallen weiterhin zu den veröffentlichten Tarifen an.

AWS CloudTrail Management-Ereignisse sind für die folgenden Profile verfügbar:

- AWS Konto
- AWS Nutzer
- AWS Rolle
- AWS Rolle Sitzung
- Amazon EC2-Instance
- Amazon-S3-Bucket
- IP-Adresse

- Kubernetes-Cluster
- Kubernetes-Pod
- Kubernetes-Thema
- IAM-Rolle
- IAM-Rollensitzung
- IAM-Benutzer

Amazon VPC Flow Logs sind für die folgenden Profile verfügbar:

- Amazon EC2-Instance
- Kubernetes-Pod

Eine Demonstration der Integration von Amazon Detective mit Amazon Security Lake mithilfe der Detective-Konsole finden Sie im folgenden Video: [Amazon Detective-Integration mit Amazon Security Lake — So verwenden Sie](#) -->

Zur Abfrage von Rohprotokollen für ein AWS-Konto

1. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich Suche und suchen Sie dann nach einem AWS account.
3. Wählen Sie im Abschnitt Gesamtes API-Aufrufvolumen die Option Details zur Rahmenzeit anzeigen.
4. Von hier aus können Sie mit der Abfrage von Rohprotokollen beginnen.

Detective > Search > AwsAccount/714603721603

714603721603
AWS account [Info](#)

Scope time [Info](#)
12/21/2023 18:00 UTC > 12/22/2023 18:00 UTC

Activity for time window: 12/21/2023 18:00 UTC - 12/22/2023 18:00 UTC [✎](#)

[Query raw logs](#)

[Observed IP addresses](#) | [API method by service](#) | [Resource](#)

< 1 >

IP address ▾	Successful calls ▾	Failed calls ▾	Location ▾	Actions
▶ [redacted]	6	2	[redacted]	
▶ [redacted]	2	1	-	
▶ [redacted]	1	0	[redacted]	

In der Vorschautabelle für Rohprotokolle können Sie die Protokolle und Ereignisse anzeigen, die durch Abfragen von Daten aus Security Lake abgerufen wurden. Weitere Informationen zu den unbearbeiteten Ereignisprotokollen finden Sie in den in Amazon Athena angezeigten Daten.

Raw log preview: CloudTrail

View raw event logs that were retrieved by querying data from Security Lake. For more details about the raw event logs, you can view the data displayed in Athena.

Raw log preview (500+) < 1 2 3 4 5 6 7 ... 50 >

date_time ▾	requestor_arn ▾	account_id ▾	region ▾	source_ip ▾	service ▾	apiL
2023-12-22 09:58:38.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	s3.amazonaws.com	Getf
2023-12-22 09:59:49.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	sts.amazonaws.com	Assu
2023-12-22 10:00:13.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	ec2.amazonaws.com	Desc
2023-12-22 10:00:13.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	sts.amazonaws.com	Assu
2023-12-22 10:00:13.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	iam.amazonaws.com	Getf
2023-12-22 10:00:13.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	sts.amazonaws.com	Assu
2023-12-22 10:00:13.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	sts.amazonaws.com	GetC
2023-12-22 10:00:13.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	autoscaling.amazonaws.com	Desc
2023-12-22 10:00:14.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	ec2.amazonaws.com	Desc
2023-12-22 10:00:14.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	ec2.amazonaws.com	Desc

Close

Cancel query request

See results in Athena [↗](#)

Download results

In der Tabelle „Rohdatenprotokolle abfragen“ können Sie die Abfrageanfrage stornieren, Ergebnisse in Amazon Athena anzeigen und Ergebnisse als Datei mit kommagetrennten Werten (.csv) herunterladen.

Wenn Sie Protokolle in Detective sehen, die Abfrage aber keine Ergebnisse lieferte, kann das aus den folgenden Gründen passieren.

- Rohprotokolle werden möglicherweise in Detective verfügbar, bevor sie in den Security-Lake-Protokolltabellen angezeigt werden. Bitte versuchen Sie es später erneut.
- In Security Lake fehlen möglicherweise Protokolle. Wenn Sie über einen längeren Zeitraum gewartet haben, deutet dies darauf hin, dass Protokolle in Security Lake fehlen. Wenden Sie sich an Ihren Security-Lake-Administrator, um das Problem zu beheben.

Beispiele

- [Fragen Sie Rohprotokolle für eine AWS Rolle ab](#)
- [Rohprotokolle für einen Amazon EKS-Cluster abfragen](#)
- [Abfragen von Rohprotokollen für eine Amazon-EC2-Instance](#)

Fragen Sie Rohprotokolle für eine AWS Rolle ab

Wenn Sie die Aktivität einer AWS Rolle in einer neuen Geolokalisierung verstehen möchten, können Sie dies in der Detective-Konsole tun.

Abfragen von Rohprotokollen für eine AWS-Rolle

1. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Notieren Sie sich auf der Seite Detective Summary New Observed Geolocations die Rolle. AWS
3. Wählen Sie im Navigationsbereich Suche und suchen Sie nach der AWS `role`.
4. Erweitern Sie für die AWS Rolle die Ressource, sodass die spezifischen API-Aufrufe angezeigt werden, die von dieser Ressource von dieser IP-Adresse aus gesendet wurden.
5. Wählen Sie das Lupensymbol neben dem API-Aufruf, den Sie untersuchen möchten, um die Tabelle mit der Vorschau des Rohprotokolls zu öffnen.

Activity for time window: 

Q Query raw logs

Observed IP addresses | **API method by service** | Resource

< 1 >

IP address ▾	Successful calls ▾	Failed calls ▾	Location ▾	Actions
▶ <input type="text"/>	289	284	-	
▶ <input type="text"/>	63	0	<input type="text"/>	
▶ <input type="text"/>	42	0	<input type="text"/>	
▶ <input type="text"/>	21	0	<input type="text"/>	

Rohprotokolle für einen Amazon EKS-Cluster abfragen

1. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Navigieren Sie auf der Seite Detective Summary im Abschnitt Container-Cluster mit den meisten erstellten Pods zu einem Amazon EKS-Cluster.
3. Wählen Sie auf der Seite mit den Amazon EKS-Cluster-Details die Registerkarte Kubernetes-API-Aktivität aus.
4. Wählen Sie im Abschnitt Allgemeine Kubernetes-API-Aktivität, an der dieser Amazon EKS-Cluster beteiligt ist, die Option Details anzeigen für den Geltungsbereich aus.
5. Von hier aus können Sie mit der Abfrage von Rohprotokollen beginnen.

Abfragen von Rohprotokollen für eine Amazon-EC2-Instance

1. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich Suche und suchen Sie dann nach einem Amazon EC2 instance.
3. Wählen Sie im Abschnitt Gesamtvolumen des VPC-Durchflusses das Lupensymbol neben dem API-Aufruf, den Sie untersuchen möchten, um die Tabelle mit der Vorschau des Rohprotokolls zu öffnen.
4. Von hier aus können Sie mit der Abfrage von Rohprotokollen beginnen.

Activity for time window: 11/21/2023 11:00 (UTC-08:00) - 11/22/2023 11:00 (UTC-08:00) ↗

Toggle overall traffic

Query raw logs

Filter

< 1 2 3 4 5 6 7 ... 888 >

<input type="checkbox"/>	IP address ▾	Local port ▾	Remote port ▾	Inbound traffic ▾	Outbound traffic ▾	Protocol ▾	Directionality ▾	Accept / Reject ▾	Actions
<input type="checkbox"/>		22	-	44.7 kB	57.7 kB	TCP	Inbound	Accept	<input type="checkbox"/>
<input type="checkbox"/>		22	-	240 B	480 B	TCP	Inbound	Accept	<input type="checkbox"/>
<input type="checkbox"/>		22	-	61.1 kB	75 kB	TCP	Inbound	Accept	<input type="checkbox"/>
<input type="checkbox"/>		22	-	59.6 kB	70.8 kB	TCP	Inbound	Accept	<input type="checkbox"/>
<input type="checkbox"/>		22	-	240 B	540 B	TCP	Inbound	Accept	<input type="checkbox"/>

In der Vorschautabelle für Rohprotokolle können Sie die Protokolle und Ereignisse anzeigen, die durch Abfragen von Daten aus Security Lake abgerufen wurden. Weitere Informationen zu den unbearbeiteten Ereignisprotokollen finden Sie in den in Amazon Athena angezeigten Daten.

In der Tabelle „Rohdatenprotokolle abfragen“ können Sie die Abfrageanfrage stornieren, Ergebnisse in Amazon Athena anzeigen und Ergebnisse als Datei mit kommagetrennten Werten (.csv) herunterladen.

Sicherheit in Amazon Detective

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können.

Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der [AWS -Compliance-Programme](#) regelmäßig.

Weitere Informationen zu den für Amazon Detective geltenden Compliance-Programmen finden Sie unter [Im Rahmen des Compliance-Programms zugelassene AWS -Services](#).

- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der geteilten Verantwortung bei der Verwendung von Detective einsetzen können. Die folgenden Themen veranschaulichen, wie Sie Detective zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie lernen auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre Detective-Ressourcen zu überwachen und zu sichern.

Inhalt

- [Datenschutz in Amazon Detective](#)
- [Identitäts- und Zugriffsverwaltung für Amazon Detective](#)
- [Protokollierung und Überwachung in Amazon Detective](#)
- [Compliance-Validierung für Amazon Detective](#)
- [Ausfallsicherheit bei Amazon Detective](#)
- [Sicherheit der Infrastruktur in Amazon Detective](#)
- [Best Practices für die Sicherheit in Amazon Detective](#)

Datenschutz in Amazon Detective

Das AWS [Modell](#) der gilt für den Datenschutz in Amazon Detective. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter [Häufig gestellte Fragen zum Datenschutz](#). Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag [AWS -Modell der geteilten Verantwortung und in der DSGVO](#) im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-2](#).

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Detective oder anderen zusammenarbeiten und die Konsole, die API oder AWS SDKs AWS-Services verwenden. AWS CLI Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine

Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Detective verschlüsselt alle Daten, die im Ruhezustand und während der Übertragung verarbeitet und gespeichert werden.

Inhalt

- [Schlüsselverwaltung für Amazon Detective](#)

Schlüsselverwaltung für Amazon Detective

Da Detective keine persönlich identifizierbaren Kundendaten speichert, verwendet es Von AWS verwaltete Schlüssel.

Diese Art von KMS-Schlüssel kann für mehrere Konten verwendet werden. Die [Beschreibung der AWS eigenen Schlüssel finden Sie im AWS Key Management Service Entwicklerhandbuch](#).

Diese Art von KMS-Schlüssel wird automatisch jedes Jahr (ungefähr 365 Tage) rotiert. Die [Beschreibung der Schlüsselrotation finden Sie im AWS Key Management Service Entwicklerhandbuch](#).

Identitäts- und Zugriffsverwaltung für Amazon Detective

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert (berechtigt) werden kann, Detective-Ressourcen zu nutzen. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Inhalt

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [So funktioniert Amazon Detective mit IAM](#)
- [Beispiele für identitätsbasierte Amazon-Detective-Richtlinien](#)
- [AWS verwaltete Richtlinien für Amazon Detective](#)
- [Verwenden von serviceverknüpften Rollen für Detective](#)
- [Fehlerbehebung für Amazon-Detective-Identität und -Zugriff](#)

Zielgruppe

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

Service-Benutzer – Wenn Sie den Detective-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere Detective-Features ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie auf ein Feature in Detective nicht zugreifen können, siehe [Fehlerbehebung für Amazon-Detective-Identität und -Zugriff](#).

Service-Administrator – Wenn Sie in Ihrem Unternehmen für -Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf Detective. Es ist Ihre Aufgabe, festzulegen, auf welche Detective-Features und Ressourcen Ihre Servicenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Detective verwenden kann, finden Sie unter [So funktioniert Amazon Detective mit IAM](#).

IAM-Administrator – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Detective verfassen können. Beispiele für identitätsbasierte Detective-Richtlinien, die Sie in IAM verwenden können, finden Sie unter [Beispiele für identitätsbasierte Amazon-Detective-Richtlinien](#).

Authentifizierung mit Identitäten

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

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

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

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

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

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität innerhalb von Ihnen AWS-Konto, die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter [Regelmäßiges](#)

[Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Eine [IAM-Gruppe](#) ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

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

IAM-Rollen

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

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

- **Verbundbenutzerzugriff** – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter [Erstellen von Rollen für externe Identitätsanbieter](#) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze](#) im AWS IAM Identity Center -Benutzerhandbuch.
- **Temporäre IAM-Benutzerberechtigungen** – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.

- **Kontoübergreifender Zugriff** – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch](#).
- **Serviceübergreifender Zugriff** — Einige verwenden Funktionen in anderen. AWS-Services Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
- **Forward Access Sessions (FAS)** — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).
- **Servicerolle** – Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.
- **Dienstbezogene Rolle** — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- **Anwendungen, die auf Amazon EC2 ausgeführt werden** — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie

ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter [Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden](#) im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter [Erstellen einer IAM-Rolle \(anstatt eines Benutzers\)](#) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

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

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern,

welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter [Auswahl zwischen verwalteten und eingebundenen Richtlinien](#) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

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

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter [Zugriffskontrollliste \(ACL\) – Übersicht](#) (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- **Berechtigungsgrenzen** – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im IAM-Benutzerhandbuch.
- **Service Control Policies (SCPs)** — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter [Funktionsweise von SCPs](#) im AWS Organizations -Benutzerhandbuch.
- **Sitzungsrichtlinien** – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird,

ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

So funktioniert Amazon Detective mit IAM

Benutzer und Rollen besitzen standardmäßig keine Berechtigungen zum Erstellen oder Ändern von Amazon-Detective-Ressourcen. Sie können auch keine Aufgaben mit der AWS Management Console, AWS CLI, oder AWS API ausführen. Ein Detective-Administrator muss über AWS Identity and Access Management (IAM-) Richtlinien verfügen, die IAM-Benutzern und -Rollen die Erlaubnis gewähren, bestimmte API-Operationen mit den angegebenen Ressourcen auszuführen, die sie benötigen. Der Administrator muss diese Richtlinien anschließend dem Prinzipal anfügen, der diese Berechtigungen benötigt.

Detective verwendet identitätsbasierte IAM-Richtlinien, um Berechtigungen für die folgenden Benutzer- und Aktionstypen zu gewähren:

- **Administratorkonten** – Das Administratorkonto ist der Besitzer eines Verhaltensdiagramms, das Daten aus seinem Konto verwendet. Administratorkonten können Mitgliedskonten einladen, ihre Daten zum Verhaltensdiagramm beizutragen. Das Administratorkonto kann das Verhaltensdiagramm auch zur Triage und Untersuchung der Ergebnisse und Ressourcen im Zusammenhang mit diesen Konten verwenden.

Sie können Richtlinien einrichten, die es anderen Benutzern als dem Administratorkonto ermöglichen, verschiedene Arten von Aufgaben auszuführen. Beispielsweise verfügt ein Benutzer mit einem Administratorkonto möglicherweise nur über Berechtigungen zur Verwaltung von Mitgliedskonten. Ein anderer Benutzer ist möglicherweise nur berechtigt, das Verhaltensdiagramm für Untersuchungen zu verwenden.

- **Mitgliedskonten** – Ein Mitgliedskonto ist ein Konto, das aufgefordert wird, Daten zu einem Verhaltensdiagramm beizutragen. Ein Mitgliedskonto reagiert auf eine Einladung. Nachdem ein Mitgliedskonto eine Einladung angenommen hat, kann es sein Konto aus dem Verhaltensdiagramm entfernen.

Einen allgemeinen Überblick darüber, wie Detective und andere mit IAM AWS-Services arbeiten, finden Sie im IAM-Benutzerhandbuch unter [Richtlinien auf der Registerkarte JSON erstellen](#).

Detective-Richtlinien auf Identitätsbasis

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. Detective unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel.

Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

Aktionen

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

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

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

Richtlinienanweisungen müssen entweder ein `Action`- oder ein `NotAction`-Element enthalten. Das Element `Action` listet die Aktionen auf, die im Rahmen der Richtlinie zulässig sind. Das Element `NotAction` listet die Aktionen auf, die nicht zulässig sind.

Die für Detective definierten Aktionen spiegeln Aufgaben wider, die Sie mit Detective ausführen können. Richtlinienaktionen in Detective haben das folgende Präfix: `detective:`.

Um beispielsweise die Berechtigung zu erteilen, die `CreateMembers` API-Operation zum Laden von Mitgliedskonten zu einem Verhaltensdiagramm zu verwenden, fügen Sie die Aktion `detective:CreateMembers` in deren Richtlinie ein.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata: Für ein Mitgliedskonto umfasst die Richtlinie beispielsweise eine Reihe von Aktionen im Zusammenhang mit der Verwaltung einer Einladung:

```
"Action": [  
  "detective:ListInvitations",  
  "detective:AcceptInvitation",  
  "detective:RejectInvitation",  
  "detective:DisassociateMembership"  
]
```

Sie können Platzhalter (*) verwenden, um mehrere Aktionen anzugeben. Um beispielsweise die in ihrem Verhaltensdiagramm verwendeten Daten zu verwalten, müssen Administratorkonten in Detective in der Lage sein, die folgenden Aufgaben auszuführen:

- Sehen Sie sich ihre Liste der Mitgliedskonten an (`ListMembers`).
- Informieren Sie sich über ausgewählte Mitgliedskonten (`GetMembers`).
- Laden Sie Mitgliedskonten zu ihrem Verhaltensdiagramm ein (`CreateMembers`).
- Entfernen Sie Mitglieder aus ihrem Verhaltensdiagramm (`DeleteMembers`).

Anstatt diese Aktionen separat aufzulisten, können Sie Zugriff auf alle Aktionen gewähren, die mit dem Wort `Members` enden. Die Richtlinie dafür könnte die folgende Aktion beinhalten:

```
"Action": "detective:*Members"
```

Eine Liste der Detective-Aktionen finden Sie unter [Von Amazon Detective definierte Aktionen](#) in der Service-Autorisierungs-Referenz.

Ressourcen

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

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein `Resource` oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen [Amazon-Ressourcennamen \(ARN\)](#) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

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

```
"Resource": "*" 
```

Weitere Informationen zum Format von ARNs finden Sie unter [Amazon Resource Names \(ARNs\) und AWS Service Namespaces](#).

Für Detective ist der einzige Ressourcentyp das Verhaltensdiagramm. Die Ressource Verhaltensdiagramm in Detective hat den folgenden ARN:

```
arn:aws:detective:${Region}:${AccountId}:graph:${GraphId}
```

Ein Verhaltensdiagramm hat beispielsweise folgende Werte:

- Die Region für das Verhaltensdiagramm ist `us-east-1`.
- Die Konto-ID für die Administratorkonto-ID lautet `111122223333`.
- Die Diagramm-ID des Verhaltensdiagramms lautet `027c7c4610ea4aacf0b883093cab899`.

Um dieses Verhaltensdiagramm in einer `Resource`-Anweisung zu identifizieren, würden Sie den folgenden ARN verwenden:

```
"Resource": "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacf0b883093cab899" 
```

Wenn Sie mehrere Ressourcen in einer `Resource`-Anweisung angeben möchten, trennen Sie sie durch Kommata.

```
"Resource": [
  "resource1",
  "resource2"
]
```

Beispielsweise kann dasselbe AWS Konto in mehr als einem Verhaltensdiagramm als Mitgliedskonto eingeladen werden. In der Richtlinie für dieses Mitgliedskonto würden in der `Resource`-Erklärung die Verhaltensdiagramme aufgeführt, zu denen das Mitglied eingeladen wurde.

```
"Resource": [  
  "arn:aws:detective:us-  
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",  
  "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bb1uw1d164680eby416"  
]
```

Einige Detective-Aktionen, wie das Erstellen eines Verhaltensdiagramms, das Auflisten von Verhaltensdiagrammen und das Auflisten von Einladungen zum Verhaltensdiagramm, werden nicht für ein bestimmtes Verhaltensdiagramm ausgeführt. Für diese Aktionen muss die Resource-Anweisung den Platzhalter (*) verwenden.

```
"Resource": "*"
```

Bei Aktionen mit Administratorkonten überprüft Detective immer, ob der Benutzer, der die Anfrage stellt, dem Administratorkonto für das betroffene Verhaltensdiagramm angehört. Bei Aktionen mit Mitgliedskonten überprüft Detective immer, ob der Benutzer, der die Anfrage stellt, dem Mitgliedskonto angehört. Selbst wenn eine IAM-Richtlinie Zugriff auf ein Verhaltensdiagramm gewährt, kann der Benutzer die Aktion nicht ausführen, wenn der Benutzer nicht dem richtigen Konto angehört.

Für alle Aktionen, die auf einem bestimmten Verhaltensdiagramm ausgeführt werden, sollte die IAM-Richtlinie den Diagramm-ARN enthalten. Der Diagramm-ARN kann später hinzugefügt werden. Wenn beispielsweise ein Konto Detective zum ersten Mal aktiviert, gewährt die anfängliche IAM-Richtlinie Zugriff auf alle Detective-Aktionen, wobei der Platzhalter für den Diagramm-ARN verwendet wird. Auf diese Weise kann der Benutzer sofort damit beginnen, Mitgliedskonten für sein Verhaltensdiagramm zu verwalten und Untersuchungen durchzuführen. Nachdem das Verhaltensdiagramm erstellt wurde, können Sie die Richtlinie aktualisieren, um den Diagramm-ARN hinzuzufügen.

Bedingungsschlüssel

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

Das Element `Condition` (oder `Condition block`) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die [Bedingungsoperatoren](#) verwenden, z. B. `ist gleich oder kleiner als`, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

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

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

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [Kontextschlüssel für AWS globale Bedingungen](#) im IAM-Benutzerhandbuch.

Detective definiert keinen eigenen Satz von Bedingungsschlüsseln. Sie unterstützt die Verwendung einiger globaler Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [AWS Globale Bedingungskontextschlüssel](#) im IAM-Benutzerhandbuch.

Informationen dazu, für welche Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter [Von Amazon Detective definierte Aktionen](#).

Beispiele

Beispiele für identitätsbasierte Detective-Richtlinien finden Sie unter [Beispiele für identitätsbasierte Amazon-Detective-Richtlinien](#).

Ressourcenbasierte Detective-Richtlinien (nicht unterstützt)

Detective unterstützt keine ressourcenbasierten Richtlinien.

Autorisierung auf der Grundlage von Detective Behavior Diagramm-Tags

Jedem Verhaltensdiagramm können Tag-Werte zugewiesen werden. Sie können diese Tagwerte in Bedingungsanweisungen verwenden, um den Zugriff auf das Verhaltensdiagramm zu verwalten.

Die Bedingungsanweisung für einen Tag-Wert verwendet das folgende Format.

```
{"StringEquals":{"aws:ResourceTag/<tagName>": "<tagValue>"}}
```

Verwenden Sie beispielsweise den folgenden Code, um eine Aktion zuzulassen oder abzulehnen, wenn der Wert des Department-Tags Finance lautet.

```
{"StringEquals":{"aws:ResourceTag/Department": "Finance"}}
```

Beispiele für Richtlinien, die Ressourcen-Tag-Werte verwenden, finden Sie unter [the section called “Administratorkonto: Zugriff auf der Grundlage von Tag-Werten einschränken”](#).

Detective IAM-Rollen

Eine [IAM-Rolle](#) ist eine Entität in Ihrem AWS Konto, die über bestimmte Berechtigungen verfügt.

Verwenden temporärer Anmeldeinformationen mit Detective

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS API-Operationen wie [AssumeRole](#) oder [GetFederationToken](#) aufrufen.

Detective unterstützt die Verwendung temporärer Anmeldeinformationen.

Service-verknüpfte Rollen

Mit [dienstbezogenen Rollen](#) können AWS Dienste auf Ressourcen in anderen Diensten zugreifen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Detective-Rollen finden Sie unter [the section called “Verwenden von serviceverknüpften Rollen”](#).

Service rollen (nicht unterstützt)

Dieses Feature ermöglicht einem Service das Annehmen einer [Service rolle](#) in Ihrem Namen. Diese Rolle gewährt dem Service Zugriff auf Ressourcen in anderen Diensten, um eine Aktion in Ihrem Namen auszuführen. Service rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Konto. Dies bedeutet, dass ein IAM-Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

Detective unterstützt keine Service rollen.

Beispiele für identitätsbasierte Amazon-Detective-Richtlinien

IAM-Benutzer besitzen standardmäßig keine Berechtigungen zum Erstellen oder Ändern von Detective-Ressourcen. Sie können auch keine Aufgaben mithilfe der AWS API, der AWS Management Console, der AWS CLI, oder ausführen.

Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den IAM-Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter [Erstellen von Richtlinien auf der JSON-Registerkarte](#) im IAM-Benutzerhandbuch.

Themen

- [Bewährte Methoden für Richtlinien](#)
- [Verwenden der Detective-Konsole](#)
- [Benutzern die Berechtigung zur Anzeige eigener Berechtigungen erteilen](#)
- [Administratorkonto: Verwaltung der Mitgliedskonten in einem Verhaltensdiagramm](#)
- [Administratorkonto: Verwendung eines Verhaltensdiagramms zur Untersuchung](#)
- [Mitgliedskonto: Verwaltung von Einladungen und Mitgliedschaften im Verhaltensdiagramm](#)
- [Administratorkonto: Zugriff auf der Grundlage von Tag-Werten einschränken](#)

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Detective-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien

definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter [AWS -verwaltete Richtlinien](#) oder [AWS -verwaltete Richtlinien für Auftrags-Funktionen](#) im IAM-Benutzerhandbuch.

- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter [Richtlinien und Berechtigungen in IAM](#) im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: Bedingung](#) im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter [Richtlinienvvalidierung zum IAM Access Analyzer](#) im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter [Konfigurieren eines MFA-geschützten API-Zugriffs](#) im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Bewährte Methoden für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

Verwenden der Detective-Konsole

Um die Amazon-Detective-Konsole verwenden zu können, muss der Benutzer oder die Rolle Zugriff auf die Aktionen haben, die den jeweiligen Aktionen in der API entsprechen.

Um Detective zu aktivieren und Administratorkonto für ein Verhaltensdiagramm zu werden, muss dem Benutzer oder der Rolle die Berechtigung für die Aktion `CreateGraph` erteilt werden.

Um mit der Detective-Konsole Aktionen eines Administratorkontos ausführen zu können, muss dem Benutzer oder der Rolle die Berechtigung für die Aktion `ListGraphs` erteilt werden.

Dadurch wird die Berechtigung zum Abrufen der Verhaltensdiagramme erteilt, für die ihr Konto ein Administratorkonto ist. Außerdem muss ihnen die Berechtigung erteilt werden, bestimmte Administratorkonto-Aktionen durchzuführen.

Die grundlegendsten Aktionen für Administratorkonten bestehen darin, eine Liste der Mitgliedskonten in einem Verhaltensdiagramm anzuzeigen und das Verhaltensdiagramm zur Untersuchung zu verwenden.

- Um die Liste der Mitgliedskonten in einem Verhaltensdiagramm anzuzeigen, muss dem Prinzipal die entsprechende Genehmigung für die Aktion `ListMembers` erteilt werden.
- Um eine Untersuchung in einem Verhaltensdiagramm durchführen zu können, muss dem Prinzipal die Genehmigung für die Aktion `SearchGraph` erteilt werden.

Um mit der Detective-Konsole Aktionen eines Mitgliedskontos ausführen zu können, muss dem Benutzer oder der Rolle die entsprechende Berechtigung für die Aktion `ListInvitations` erteilt werden. Dadurch wird die Berechtigung zum Anzeigen von Einladungen in Verhaltensdiagrammen erteilt. Anschließend kann ihnen die Erlaubnis für bestimmte Aktionen im Mitgliedskonto erteilt werden.

Benutzern die Berechtigung zur Anzeige eigener Berechtigungen erteilen

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

```
{  
  "Version": "2012-10-17",
```

```

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

```

Administratorkonto: Verwaltung der Mitgliedskonten in einem Verhaltensdiagramm

Diese Beispielrichtlinie richtet sich an Benutzer von Administratorkonten, die nur für die Verwaltung der im Verhaltensdiagramm verwendeten Mitgliedskonten verantwortlich sind. Die Richtlinie ermöglicht dem Benutzer auch das Anzeigen der Nutzungsinformationen und das Deaktivieren von Detective. Die Richtlinie gewährt nicht die Erlaubnis, das Verhaltensdiagramm für Untersuchungen zu verwenden.

```

{"Version":"2012-10-17",
 "Statement":[
  {
    "Effect":"Allow",

```

```

    "Action":
["detective:ListMembers","detective:CreateMembers","detective:DeleteMembers","detective:DeleteG
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacadf0b883093cab899"
  },
  {
    "Effect":"Allow",
    "Action":["detective:CreateGraph","detective:ListGraphs"],
    "Resource": "*"
  }
]
}

```

Administratorkonto: Verwendung eines Verhaltensdiagramms zur Untersuchung

Diese Beispielrichtlinie ist für Benutzer von Administratorkonten vorgesehen, die das Verhaltensdiagramm nur zur Untersuchung verwenden. Sie können die Liste der Mitgliedskonten im Verhaltensdiagramm nicht anzeigen oder bearbeiten.

```

{"Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":["detective:SearchGraph"],
      "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacadf0b883093cab899"
    },
    {
      "Effect":"Allow",
      "Action":["detective:ListGraphs"],
      "Resource": "*"
    }
  ]
}

```

Mitgliedskonto: Verwaltung von Einladungen und Mitgliedschaften im Verhaltensdiagramm

Diese Beispielrichtlinie richtet sich an Benutzer, die zu einem Mitgliedskonto gehören. Im Beispiel gehört das Mitgliedskonto zu zwei Verhaltensdiagrammen. Die Richtlinie gewährt die Erlaubnis, auf Einladungen zu antworten und das Mitgliedskonto aus dem Verhaltensdiagramm zu entfernen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation", "detective:RejectInvitation", "detective:DisassociateMembership"
      ],
      "Resource": [
        "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
        "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bb1uw1d164680eby416"
      ]
    },
    {
      "Effect": "Allow",
      "Action": ["detective:ListInvitations"],
      "Resource": "*"
    }
  ]
}
```

Administratorkonto: Zugriff auf der Grundlage von Tag-Werten einschränken

Die folgende Richtlinie ermöglicht es dem Benutzer, ein Verhaltensdiagramm zur Untersuchung zu verwenden, wenn das SecurityDomain-Tag des Verhaltensdiagramms mit dem SecurityDomain-Tag des Benutzers übereinstimmt.

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Action": ["detective:SearchGraph"],
    "Resource": "arn:aws:detective:*:*:graph:*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/SecurityDomain": "aws:PrincipalTag/SecurityDomain"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": ["detective:ListGraphs"],
```

```
    "Resource": "*"
  } ]
}
```

Die folgende Richtlinie verhindert, dass Benutzer ein Verhaltensdiagramm für Untersuchungen verwenden, wenn der Wert des SecurityDomain-Tags für das Verhaltensdiagramm Finance lautet.

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Deny",
    "Action": [ "detective:SearchGraph" ],
    "Resource": "arn:aws:detective:*:*:graph:*",
    "Condition": {
      "StringEquals": { "aws:ResourceTag/SecurityDomain": "Finance" }
    }
  } ]
}
```

AWS verwaltete Richtlinien für Amazon Detective

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

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie [kundenverwaltete Richtlinien](#) definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter [Von AWS verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AmazonDetectiveFullAccess

Sie können die AmazonDetectiveFullAccess-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen, die einem Prinzipal vollen Zugriff auf alle Amazon-Detective-Aktionen erlauben. Sie können diese Richtlinie einem Prinzipalen zuweisen, bevor dieser Detective für sein Konto aktiviert. Sie muss auch an die Rolle angehängt werden, mit der die Python-Skripts in Detective ausgeführt werden, um ein Verhaltensdiagramm zu erstellen und zu verwalten.

Prinzipale mit diesen Berechtigungen können Mitgliedskonten verwalten, ihrem Verhaltensdiagramm Tags hinzufügen und Detective für Ermittlungen verwenden. Sie können GuardDuty Ergebnisse auch archivieren. Die Richtlinie bietet Berechtigungen, die die Detective-Konsole benötigt, um Kontonamen für Konten anzuzeigen, die sich in befinden AWS Organizations.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `detective` – Ermöglicht Prinzipalen vollen Zugriff auf alle Detective-Aktionen.
- `organizations` – Ermöglicht Prinzipalen das Abrufen von AWS Organizations -Informationen über die Konten in einer Organisation. Wenn ein Konto zu einer Organisation gehört, ermöglichen diese Berechtigungen der Detective-Konsole, zusätzlich zu den Kontonummern auch Kontonamen anzuzeigen.
- `guardduty`— Ermöglicht es den Schulleitern, GuardDuty Ergebnisse aus Detective abzurufen und zu archivieren.
- `securityhub` – Ermöglicht es Prinzipalen, Security Hub-Erkenntnisse aus Detective heraus abzurufen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:*",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
    },
  ],
}
```

```

    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "guardduty:ArchiveFindings"
    ],
    "Resource": "arn:aws:guardduty:*:*:detector/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "guardduty:GetFindings",
      "guardduty:ListDetectors"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "securityHub:GetFindings"
    ],
    "Resource": "*"
  }
]
}

```

AWS verwaltete Richtlinie: AmazonDetectiveMemberAccess

Sie können die AmazonDetectiveMemberAccess-Richtlinie auch Ihren IAM-Entitäten anfügen.

Diese Richtlinie gewährt Mitgliedern Zugriff auf Amazon Detective und begrenzten Zugriff auf die Konsole.

Mit dieser Richtlinie können Sie:

- Sich Einladungen zur Detective Diagramm-Mitgliedschaft ansehen und diese Einladungen akzeptieren oder ablehnen.
- Auf der Seite Nutzung sehen, wie Ihre Aktivität in Detective zu den Kosten für die Nutzung dieses Dienstes beiträgt.

- Ihre Mitgliedschaft in einem Diagramm kündigen.

Diese Richtlinie gewährt Berechtigungen, die einen schreibgeschützten Zugriff auf die Detective-Konsole erlauben.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `detective` – Ermöglicht Mitgliedern den Zugriff auf Detective.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource": "*"
    }
  ]
}
```

Von AWS verwaltete Richtlinie: `AmazonDetectiveInvestigatorAccess`

Sie können die `AmazonDetectiveInvestigatorAccess`-Richtlinie auch Ihren IAM-Entitäten hinzufügen.

Diese Richtlinie gewährt Ermittlern Zugriff auf den Detective Service und bereichsspezifischen Zugriff auf die Abhängigkeiten der Benutzeroberfläche der Detective-Konsole. Diese Richtlinie gewährt IAM-Benutzern und IAM-Rollen Berechtigungen zur Aktivierung von Untersuchungen in Detective. Mithilfe eines Untersuchungsberichts, der Analysen und Erkenntnisse in Sicherheitsindikatoren bietet, können Sie Indikatoren für eine Kompromittierung ermitteln, z. B. Erkenntnisse. Der Bericht ist nach Schweregrad geordnet, der mithilfe von Verhaltensanalyse und Machine Learning von Detective ermittelt wird. Sie können den Bericht verwenden, um die Behebung von Ressourcen zu priorisieren.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `detective` – Ermöglicht Prinzipalen die Untersuchung des Zugriffs auf Detective-Aktionen, die Aktivierung von Untersuchungen in Detective und die Übersicht von Erkenntnisgruppen.
- `guardduty`— Ermöglicht es den Schulleitern, GuardDuty Ergebnisse aus Detective abzurufen und zu archivieren.
- `securityhub` – Ermöglicht es Prinzipalen, Security Hub-Erkenntnisse aus Detective heraus abzurufen.
- `organizations`— Ermöglicht Prinzipalen das Abrufen von Informationen über die Konten in einer Organisation von. AWS Organizations Wenn ein Konto zu einer Organisation gehört, ermöglichen diese Berechtigungen der Detective-Konsole, zusätzlich zu den Kontonummern auch Kontonamen anzuzeigen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DetectivePermissions",
      "Effect": "Allow",
      "Action": [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
```

```
    "detective:GetUsageInformation",
    "detective:ListDatasourcePackages",
    "detective:ListGraphs",
    "detective:ListHighDegreeEntities",
    "detective:ListInvitations",
    "detective:ListMembers",
    "detective:ListOrganizationAdminAccount",
    "detective:ListTagsForResource",
    "detective:SearchGraph",
    "detective:StartInvestigation",
    "detective:GetInvestigation",
    "detective:ListInvestigations",
    "detective:UpdateInvestigationState",
    "detective:ListIndicators",
    "detective:InvokeAssistant"
  ],
  "Resource": "*"
},
{
  "Sid": "OrganizationsPermissions",
  "Effect": "Allow",
  "Action": [
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource": "*"
},
{
  "Sid": "GuardDutyPermissions",
  "Effect": "Allow",
  "Action": [
    "guardduty:ArchiveFindings",
    "guardduty:GetFindings",
    "guardduty:ListDetectors"
  ],
  "Resource": "*"
},
{
  "Sid": "SecurityHubPermissions",
  "Effect": "Allow",
  "Action": [
    "securityHub:GetFindings"
  ],
  "Resource": "*"
}
```

```
}  
]  
}
```

AWS verwaltete Richtlinie: AmazonDetectiveOrganizationsAccess

Sie können die AmazonDetectiveOrganizationsAccess-Richtlinie auch Ihren IAM-Entitäten anfügen.

Diese Richtlinie gewährt die Erlaubnis, Amazon Detective innerhalb einer Organisation zu aktivieren und zu verwalten. Sie können Detective unternehmensweit aktivieren und das delegierte Administratorkonto für Detective festlegen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `detective` – Ermöglicht Prinzipalen Zugriff auf alle Detective-Aktionen.
- `iam` – Gibt an, dass eine serviceverknüpfte Rolle erstellt wird, wenn Detective `EnableOrganizationAdminAccount` aufruft.
- `organizations`— Ermöglicht Prinzipalen das Abrufen von Informationen über die Konten in einer Organisation von AWS Organizations. Wenn ein Konto zu einer Organisation gehört, ermöglichen diese Berechtigungen der Detective-Konsole, zusätzlich zu den Kontonummern auch Kontonamen anzuzeigen. Ermöglicht die Integration eines AWS Dienstes, ermöglicht die Registrierung und Abmeldung des angegebenen Mitgliedskontos als delegierter Administrator und ermöglicht es Prinzipalen, delegierte Administratorkonten in anderen Sicherheitsdiensten wie Amazon Detective, Amazon GuardDuty, Amazon Macie und abzurufen. AWS Security Hub

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "detective:DisableOrganizationAdminAccount",  
        "detective:EnableOrganizationAdminAccount",  
        "detective:ListOrganizationAdminAccount"  
      ]  
    }  
  ]  
}
```

```
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": "detective.amazonaws.com"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "organizations:EnableAWSServiceAccess",
      "organizations:RegisterDelegatedAdministrator",
      "organizations:DeregisterDelegatedAdministrator"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "organizations:ServicePrincipal": [
          "detective.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:ListAccounts"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "organizations:ListDelegatedAdministrators"
    ]
  }
]
```

```
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "organizations:ServicePrincipal": [
          "detective.amazonaws.com",
          "guardduty.amazonaws.com",
          "macie.amazonaws.com",
          "securityhub.amazonaws.com"
        ]
      }
    }
  }
]
```

Von AWS verwaltete Richtlinie: AmazonDetectiveServiceLinkedRole

Sie können die AmazonDetectiveServiceLinkedRole-Richtlinie Ihren IAM-Entitäten nicht anfügen. Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen von Detective in Ihrem Namen ermöglicht. Weitere Informationen finden Sie unter [the section called "Verwenden von serviceverknüpften Rollen"](#).

Diese Richtlinie gewährt administrative Berechtigungen, die es der dienstverknüpften Rolle ermöglichen, Kontoinformationen für eine Organisation abzurufen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `organizations` – Ruft Kontoinformationen für eine Organisation ab.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount",
```

```

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

```

Detective Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Detective an, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der [Seite - Dokumentverlauf](#).

Änderung	Beschreibung	Datum
AmazonDetectiveInvestigatorAccess – Aktualisierungen bestehender Richtlinien	<p>Der AmazonDetectiveInvestigatorAccess -Richtlinie wurden die Aktionen Detective-Untersuchungen und Erkenntnisgruppen hinzugefügt.</p> <p>Diese Aktionen ermöglichen das Starten, Abrufen und Aktualisieren von Detective-Untersuchungen und das Abrufen einer Übersicht der Erkenntnisgruppen innerhalb von Detective.</p>	26. November 2023
AmazonDetectiveFullAccess und AmazonDetectiveInvestigatorAccess – Updates von vorhandenen Richtlinien	Detective hat AmazonDetectiveFullAccess und AmazonDetectiveInvestigatorAccess -Richtlinien Security Hub GetFindings - Aktionen hinzugefügt.	16. Mai 2023

Änderung	Beschreibung	Datum
	Diese Aktionen ermöglichen das Abrufen von Security Hub-Erkenntnissen aus Detective heraus.	
AmazonDetectiveOrganizationsAccess – Neue Richtlinie.	<p>Detective hat eine AmazonDetectiveOrganizationAccess -Richtlinie hinzugefügt.</p> <p>Diese Richtlinie gewährt die Erlaubnis, Detective innerhalb einer Organisation zu aktivieren und zu verwalten.</p>	02. März 2023
AmazonDetectiveMemberAccess – Neue Richtlinie.	<p>Detective hat die AmazonDetectiveMemberAccess - Richtlinie hinzugefügt.</p> <p>Diese Richtlinie gewährt Mitgliedern Zugriff auf Detective und bereichsbezogenen Zugriff auf die Abhängigkeiten der Konsolenbenutzeroberfläche.</p>	17. Januar 2023
AmazonDetectiveFullAccess – Aktualisierung auf eine bestehende Richtlinie	<p>Detective hat der AmazonDetectiveFullAccess Richtlinie GuardDuty GetFindings Aktionen hinzugefügt.</p> <p>Diese Aktionen ermöglichen das Abrufen von GuardDuty Erkenntnissen aus Detective heraus.</p>	17. Januar 2023

Änderung	Beschreibung	Datum
AmazonDetectiveInvestigator Access – Neue Richtlinie.	Detective hat die AmazonDetectiveInvestigator Access -Richtlinie hinzugefügt. Diese Richtlinie ermöglicht es dem Prinzipal, Untersuchungen in Detective durchzuführen.	17. Januar 2023
AmazonDetectiveServiceLinkedRole – Neue Richtlinie.	Detective hat eine neue Richtlinie für seine serviceverknüpfte Rolle hinzugefügt. Die Richtlinie erlaubt es der mit dem dienstverknüpften Rolle, Informationen über die Konten in einer Organisation abzurufen.	16. Dezember 2021
Detective begann, Änderungen zu verfolgen	Detective begann, Änderungen an seinen AWS verwalteten Richtlinien zu verfolgen.	10. Mai 2021

Verwenden von serviceverknüpften Rollen für Detective

Amazon Detective verwendet AWS Identity and Access Management (IAM) [serviceverknüpfte Rollen](#). Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit Detective verknüpft ist. Dienstbezogene Rollen sind von Detective vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle macht die Einrichtung von Amazon Detective einfacher, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Detective definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre Detective-Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter [AWS-Services, die mit IAM funktionieren](#). Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für Detective

Detective verwendet die dienstbezogene Rolle mit dem Namen `AWSServiceRoleForDetective`— Erlaubt Detective, in Ihrem Namen auf AWS Organizations Informationen zuzugreifen.

Die `AWSServiceRoleForDetective` dienstbezogene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `detective.amazonaws.com`

Die `AWSServiceRoleForDetective` dienstverknüpfte Rolle verwendet die verwaltete Richtlinie. [AmazonDetectiveServiceLinkedRolePolicy](#)

Einzelheiten zu Aktualisierungen der `AmazonDetectiveServiceLinkedRolePolicy` Richtlinie finden Sie unter [Amazon Detective Updates to AWS Managed Policies](#). Abonnieren Sie den RSS-Feed auf der Seite mit dem [Dokumentenverlauf von Detective](#), um automatische Benachrichtigungen über Änderungen an dieser Richtlinie zu erhalten.

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

Erstellen einer serviceverknüpften Rolle für Detective

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie das Detective-Administratorkonto für eine Organisation in der AWS Management Console, der oder der AWS API festlegen AWS CLI, erstellt Detective 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 das Detective-

Administratorkonto für eine Organisation festlegen, erstellt Detective die serviceverknüpfte Rolle wieder für Sie.

Bearbeiten einer serviceverknüpften Rolle für Detective

Detective erlaubt Ihnen nicht, die `AWSServiceRoleForDetective` serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Detective

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpften Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Note

Wenn der Detective-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es dann erneut.

Um Detective-Ressourcen zu löschen, die von `AWSServiceRoleForDetective`

1. Entfernen Sie das Detective-Administratorkonto. Siehe [the section called “Festlegen des Detective-Administratorkontos”](#).
2. Wiederholen Sie den Vorgang in jeder Region, in der Sie das Detective-Administratorkonto festgelegt haben.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die `AWSServiceRoleForDetective` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Leitfaden.

Unterstützte Regionen für serviceverknüpfte Detective-Rollen

Detective unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter [AWS Regionen und Endpunkte](#).

Fehlerbehebung für Amazon-Detective-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die beim Arbeiten mit Detective und IAM auftreten könnten. Wenn Sie bei der Arbeit mit AWS Identity and Access Management(IAM) auf Probleme mit der Zugriffsverweigerung oder ähnlichen Problemen stoßen, lesen Sie die Themen [zur Fehlerbehebung bei IAM im IAM-Benutzerhandbuch](#).

Ich bin nicht autorisiert, eine Aktion in Detective auszuführen.

Wenn Ihnen AWS Management Console mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort bereitgestellt hat.

Der folgende Beispielfehler tritt auf, wenn der mateojackson-IAM-Benutzer versucht, die Konsole zu verwenden, um eine Einladung zum Mitgliedskonto für ein Verhaltensdiagramm anzunehmen, jedoch keine `detective:AcceptInvitation`-Berechtigungen besitzt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
perform: detective:AcceptInvitation on resource: arn:aws:detective:us-
east-1:444455556666:graph:567856785678
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion `arn:aws:detective:us-east-1:444455556666:graph:567856785678` auf die Ressource `detective:AcceptInvitation` zugreifen zu können.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an Detective übergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

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

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

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

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine Detective-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob Detective diese Funktionen unterstützt, finden Sie unter [So funktioniert Amazon Detective mit IAM](#).
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter [Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto, den Sie besitzen](#).
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter [Gewähren von Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#) im IAM-Benutzerhandbuch.

- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie im IAM-Benutzerhandbuch unter [Kontenübergreifender Ressourcenzugriff in IAM](#).

Protokollierung und Überwachung in Amazon Detective

Amazon Detective ist integriert AWS CloudTrail. CloudTrail erfasst alle API-Aufrufe für Detective als Ereignisse.

Einzelheiten zur Verwendung der CloudTrail Protokollierung für Detective finden Sie unter [the section called "Detective API-Aufrufe protokollieren mit CloudTrail"](#).

Compliance-Validierung für Amazon Detective

Amazon Detective fällt in den Geltungsbereich des AWS Versicherungsprogramms. Weitere Informationen finden Sie unter [Health Information Trust Alliance Common Security Framework \(HITRUST\) CSF](#)) CSF.

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

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

AWS bietet die folgenden Ressourcen zur Unterstützung bei der Einhaltung von Vorschriften:

- [Schnellstartanleitungen für Sicherheit und Compliance](#) – In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von sicherheits- und konformitätsorientierten Basisumgebungen auf AWS angegeben.
- [Bewertung von Ressourcen anhand von Regeln](#) im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- [AWS Security Hub](#)— Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus und hilft Ihnen AWS , die Einhaltung der Sicherheitsstandards und bewährten Verfahren der Branche zu überprüfen.

Ausfallsicherheit bei Amazon Detective

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander 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](#).

Zusätzlich zur AWS globalen Infrastruktur nutzt Detective die in Amazon DynamoDB und Amazon Simple Storage Service (Amazon S3) integrierte Resilienz.

Die Detective-Architektur ist auch widerstandsfähig gegen den Ausfall einer einzelnen Availability Zone. Diese Resilienz ist in Detective integriert und erfordert keine Konfiguration.

Sicherheit der Infrastruktur in Amazon Detective

Als verwalteter Service ist Amazon Detective 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 Detective zuzugreifen. Kunden müssen Folgendes unterstützen:

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

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit [AWS](#)

[Security Token Service](#) (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Best Practices für die Sicherheit in Amazon Detective

Detective enthält eine Reihe von Sicherheitsfeatures, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

Für Detective beziehen sich die bewährten Sicherheitsmethoden auf die Verwaltung der Konten in einem Verhaltensdiagramm.

Best Practices für Administratorkonten

Wenn Sie Mitgliedskonten in Ihr Verhaltensdiagramm einladen, laden Sie nur Konten ein, die Sie beaufsichtigen.

Beschränken Sie den Zugriff auf das Verhaltensdiagramm. Wenn ein Benutzer Zugriff auf ein Verhaltensdiagramm hat, kann er alle Erkenntnisse für die Mitgliedskonten sehen. Solche Erkenntnisse können sensible Sicherheitsinformationen preisgeben.

Bewährte Methoden für Mitgliedskonten

Wenn Sie eine Einladung zu einem Verhaltensdiagramm erhalten, stellen Sie sicher, dass Sie die Quelle der Einladung überprüfen.

Überprüfen Sie die AWS Konto-ID des Administratorkontos, das die Einladung gesendet hat. Vergewissern Sie sich, dass Sie wissen, wem das Konto gehört und ob das einladende Konto einen legitimen Grund hat, Ihre Sicherheitsdaten zu überwachen.

Prognose und Überwachung der Amazon Detective-Kosten

Um Ihnen zu helfen, Ihre Detective-Aktivitäten nachzuverfolgen, werden auf der Nutzungsseite die Menge der aufgenommenen Daten und die voraussichtlichen Kosten angezeigt.

- Bei Administratorkonten werden auf der Seite Nutzung das Datenvolumen und die voraussichtlichen Kosten für das gesamte Verhaltensdiagramm angezeigt.
- Bei Mitgliedskonten werden auf der Seite Nutzung das Datenvolumen und die voraussichtlichen Kosten für ihr Konto in den Verhaltensdiagrammen angezeigt, zu denen sie beitragen.

Detective unterstützt auch die AWS CloudTrail Protokollierung.

Inhalt

- [Über die kostenlose Testversion für Verhaltensdiagramme](#)
- [Überwachung der Nutzung und Kosten für ein Verhaltensdiagramm \(Administratorkonto\)](#)
- [Überwachung von Nutzung und Kosten in Verhaltensdiagrammen \(Mitgliedskonto\)](#)
- [Wie Amazon Detective die voraussichtlichen Kosten berechnet](#)
- [Protokollieren von Amazon Detective API-Aufrufen mit AWS CloudTrail](#)

Über die kostenlose Testversion für Verhaltensdiagramme

Amazon Detective bietet eine kostenlose 30-Tage-Testversion für jedes Konto in jeder Region. Die kostenlose Testversion für ein Konto beginnt, wenn zum ersten Mal eine der folgenden Aktionen ausgeführt wird.

- Ein Konto aktiviert Detective manuell und wird zum Administratorkonto für ein Verhaltensdiagramm.
- Ein Konto wird als Detective-Administratorkonto für eine Organisation in AWS Organizations festgelegt, und Detective wird für dieses Konto zum ersten Mal aktiviert.
- Wenn Detective für das Administratorkonto bereits aktiviert war, bevor sie benannt wurden, wird für das Konto keine neue kostenlose 30-Tage-Testversion gestartet.
- Ein Konto akzeptiert eine Einladung, ein Mitgliedskonto zu werden, in einem Verhaltensdiagramm und wird als Mitgliedskonto aktiviert.
- Ein Organisationskonto wird durch das Detective-Administratorkonto als Mitgliedskonto aktiviert.

Die kostenlose Testversion läuft ab diesem Zeitpunkt 30 Tage. Dem Konto werden keine Daten in Rechnung gestellt, die in diesem Zeitraum verarbeitet wurden. Nach Ablauf der Testphase beginnt Detective, dem Konto die Daten in Rechnung zu stellen, die es zu Verhaltensdiagrammen beiträgt. Weitere Informationen darüber, wie Sie Ihre Detective-Aktivitäten verfolgen, die Nutzung überwachen und die voraussichtlichen Kosten einsehen können, finden Sie unter [Prognose und Überwachung der Amazon Detective-Kosten](#). Weitere Informationen zu Preisen finden Sie unter [Detective-Preise](#).

Derselbe Zeitraum von 30 Tagen wird für alle Verhaltensdiagramme in der Region verwendet. Beispielsweise ist ein Konto als Mitgliedskonto für ein Verhaltensdiagramm aktiviert. Damit wird die kostenlose 30-Tage-Testversion gestartet. Nach 10 Tagen ist das Konto für ein zweites Verhaltensdiagramm in derselben Region aktiviert. Für das zweite Verhaltensdiagramm erhält das Konto 20 Tage lang kostenlose Daten.

Die kostenlose Testversion bietet mehrere Vorteile:

- Administratorkonten können die Features und Funktionen von Detective untersuchen, um deren Wert zu überprüfen.
- Administrator- und Mitgliedskonten können die Datenmenge und die geschätzten Kosten überwachen, bevor Detective beginnt, ihnen diese in Rechnung zu stellen. Siehe [the section called “Nutzung und Kosten des Administratorkontos”](#) und [the section called “Nachverfolgung der Nutzung von Mitgliedskonten”](#).

Kostenlose Testversion für optionale Datenquellen

Detective bietet auch eine kostenlose 30-Tage-Testversion für optionale Datenquellen. Diese kostenlose Testversion ist unabhängig von der kostenlosen Testversion, die für die wichtigsten Detective-Datenquellen bereitgestellt wird, wenn Detective zum ersten Mal aktiviert wird.

Note

Wenn ein Kunde ein optionales Datenquellenpaket innerhalb von 7 Tagen nach der Aktivierung deaktiviert, führt Detective einen einmaligen automatischen Reset der kostenlosen Testversion für dieses Datenquellenpaket durch, falls es erneut aktiviert wird.

Informationen zum Aktivieren oder Deaktivieren einer optionalen Datenquelle finden Sie unter [Arten optionaler Datenquellen in Detective](#).

Überwachung der Nutzung und Kosten für ein Verhaltensdiagramm (Administratorkonto)

Amazon Detective stellt jedem Konto die Daten in Rechnung, die in jedem Verhaltensdiagramm verwendet wurden, zu dem das Konto gehört. Detective berechnet für alle Daten unabhängig von der Quelle eine gestaffelte Flatrate pro GB.

Bei Administratorkonten können Sie auf der Seite Nutzung der Detective-Konsole die Datenmenge anzeigen, die in den letzten 30 Tagen nach Datenquelle oder nach Konto aufgenommen wurde. Für Administratorkonten werden außerdem die voraussichtlichen Kosten für einen typischen Zeitraum von 30 Tagen für ihr Konto und für das gesamte Verhaltensdiagramm angezeigt.

So zeigen Sie Detective-Nutzungsinformationen an

1. Melden Sie sich bei der an AWS Management Console. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich von Detective unter Einstellungen die Option Standardeinstellungen aus.
3. Wählen Sie eine Registerkarte, um zwischen der Anzeige der Nutzung nach Datenquelle oder Nach Konto zu wählen.

Volumen der für jedes Konto aufgenommenen Daten

Das aufgenommene Volumen nach Mitgliedskonto listet die aktiven Konten im Verhaltensdiagramm auf. Mitgliedskonten, die entfernt wurden, werden nicht aufgeführt.

Für jedes Konto enthält die Liste der aufgenommenen Volumen die folgenden Informationen.

- Die AWS Konto-ID und die E-Mail-Adresse des Root-Benutzers.
- Das Datum, an dem das Konto begann, Daten zum Verhaltensdiagramm beizutragen.

Für das Administratorkonto ist dies das Datum, an dem das Konto Detective aktiviert hat.

Bei Mitgliedskonten ist dies das Datum, an dem ein Konto nach Annahme der Einladung als Mitgliedskonto aktiviert wurde.

- Das Volumen der aufgenommenen Daten aus dem Konto in den letzten 30 Tagen. Die Summe umfasst alle Quelltypen.

- Ob sich das Konto derzeit in der kostenlosen Testphase befindet. Für Konten, die sich derzeit in der kostenlosen Testphase befinden, wird in der Liste die Anzahl der verbleibenden Tage angezeigt.

Wenn sich keines der Konten in der kostenlosen Testphase befindet, wird die Spalte mit dem Status der kostenlosen Testversion nicht angezeigt.

Voraussichtliche Kosten für das Verhaltensdiagramm

Die voraussichtlichen Kosten für dieses Konto zeigen die voraussichtlichen Kosten für Daten für das Administratorkonto für 30 Tage. Die voraussichtlichen Kosten basieren auf dem durchschnittlichen täglichen Volumen für das Administratorkonto.

Important

Bei diesem Betrag handelt es sich lediglich um prognostizierte Kosten. Es werden die Gesamtkosten für die Administratorkontodaten für einen typischen Zeitraum von 30 Tagen prognostiziert. Die Prognose basiert auf der Nutzung der letzten 30 Tage. Siehe [the section called “Wie Detective die voraussichtlichen Kosten berechnet”](#).

Voraussichtliche Kosten für das Verhaltensdiagramm

Die prognostizierten Kosten aller Konten zeigen die prognostizierten Gesamtkosten für 30 Tage an Daten für das gesamte Verhaltensdiagramm. Die prognostizierten Kosten basieren auf dem durchschnittlichen Tagesvolumen für jedes Konto.

Important

Bei diesem Betrag handelt es sich lediglich um prognostizierte Kosten. Es werden die Gesamtkosten für die Verhaltensdiagrammdaten für einen typischen Zeitraum von 30 Tagen prognostiziert. Die Prognose basiert auf der Nutzung der letzten 30 Tage. In den voraussichtlichen Kosten sind keine Mitgliedskonten enthalten, die aus dem Verhaltensdiagramm entfernt wurden. Siehe [the section called “Wie Detective die voraussichtlichen Kosten berechnet”](#).

Menge der von Quellpaketen aufgenommenen Daten

Wählen Sie Nach Quellpaket, um die Menge der aufgenommenen Daten in den verschiedenen Quellpaketen, die in Ihrem Verhaltensdiagramm aktiviert sind, aufgelistet zu sehen.

Alle Konten können diese Daten für ihre eigenen Konten einsehen. Ein Administratorkonto kann zusätzliche Bereiche sehen, in denen die Nutzung nach Quellpaketen für jedes Mitglied aufgeführt ist. Mitgliedskonten, die entfernt wurden, werden nicht aufgeführt.

Detective Core

Detective Core Panels zeigen das Volumen der Daten, die in den letzten 30 Tagen aus Detective Core-Quellen (CloudTrail Logs, VPC Flow Logs und GuardDuty Ergebnisse) aufgenommen wurden.

EKS-Auditprotokolle

Die Bereiche mit den EKS-Auditprotokollen zeigen das Datenvolumen, das in den letzten 30 Tagen aus EKS-Auditprotokollquellen aufgenommen wurde. Bereiche für dieses Quellpaket sind nur verfügbar, wenn EKS-Auditprotokolle für Ihr Verhaltensdiagramm aktiviert sind.

Überwachung von Nutzung und Kosten in Verhaltensdiagrammen (Mitgliedskonto)

Amazon Detective stellt jedem Konto die Daten in Rechnung, die in jedem Verhaltensdiagramm verwendet wurden, zu dem das Konto gehört. Detective berechnet für alle Daten unabhängig von der Quelle eine gestaffelte Flatrate pro GB.

Bei Mitgliedskonten werden auf der Seite Nutzung nur das Datenvolumen und die voraussichtlichen 30-Tage-Kosten für dieses Konto angezeigt.

So zeigen Sie Detective-Nutzungsinformationen an

1. Melden Sie sich bei der an AWS Management Console. Öffnen Sie die Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Wählen Sie im Navigationsbereich von Detective unter Einstellungen die Option Standardeinstellungen aus.

Aufgenommenes Volumen für jedes Verhaltensdiagramm

Das aufgenommene Volumen dieses Kontos listet die Verhaltensdiagramme auf, zu denen das Mitgliedskonto beiträgt. Mitgliedschaften, die Sie gekündigt haben, oder Mitgliedschaften, die das Administratorkonto entfernt hat, sind nicht enthalten.

Für jedes Verhaltensdiagramm umfasst die Liste die folgenden Informationen:

- Die Kontonummer des Administratorkontos
- Das Volumen der aufgenommenen Daten aus dem Mitgliedskonto in den letzten 30 Tagen. Die Summe umfasst alle Quelltypen.
- Das Datum, an dem das Mitgliedskonto für das Verhaltensdiagramm aktiviert wurde.

Prognostizierte Kosten für alle Verhaltensdiagramme

Die prognostizierten Kosten für dieses Konto zeigen die prognostizierten Kosten für 30 Tage an Daten für das Mitgliedskonto in allen Verhaltensdiagrammen an, zu denen es beiträgt. Die voraussichtlichen Kosten basieren auf dem durchschnittlichen Tagesvolumen für das Mitgliedskonto.

Important

Bei diesem Betrag handelt es sich lediglich um prognostizierte Kosten. Es werden die Gesamtkosten für die Administratorkontodaten für einen typischen Zeitraum von 30 Tagen prognostiziert. Die Prognose basiert auf der Nutzung der letzten 30 Tage. Siehe [the section called "Wie Detective die voraussichtlichen Kosten berechnet"](#).

Wie Amazon Detective die voraussichtlichen Kosten berechnet

Um die voraussichtlichen Kostenwerte zu berechnen, die auf der Seite Nutzung angezeigt werden, geht Detective wie folgt vor.

1. Um die voraussichtlichen Kosten für ein einzelnes Konto in einem Verhaltensdiagramm zu ermitteln, geht Detective wie folgt vor.
 - a. Berechnet das durchschnittliche Volumen pro Tag. Es addiert das Datenvolumen aller aktiven Tage und dividiert dann durch die Anzahl der Tage, an denen das Konto aktiv war.

Wenn das Konto vor mehr als 30 Tagen aktiviert wurde, beträgt die Anzahl der Tage 30. Wenn das Konto vor weniger als 30 Tagen aktiviert wurde, entspricht dies der Anzahl der Tage seit dem Akzeptanzdatum.

Wenn das Konto beispielsweise vor 12 Tagen aktiviert wurde, addiert Detective das für diese 12 Tage aufgenommene Volumen und dividiert es dann durch 12.

- b. Multipliziert den Tagesdurchschnitt des Kontos mit 30. Dies ist die voraussichtliche 30-tägige Nutzung des Kontos.
 - c. Verwendet das Preismodell, um die voraussichtlichen 30-Tage-Kosten für die geplante 30-tägige Nutzung zu berechnen.
2. Um die voraussichtlichen Gesamtkosten für ein Verhaltensdiagramm zu ermitteln, geht Detective wie folgt vor:
 - a. Kombiniert die prognostizierte 30-tägige Nutzung aller Konten im Verhaltensdiagramm.
 - b. Verwendet das Preismodell, um die voraussichtlichen Kosten für 30 Tage für die gesamte geplante Nutzung von 30 Tagen zu berechnen.
 3. Um die voraussichtlichen Gesamtkosten für ein Mitgliedskonto anhand von Verhaltensdiagrammen zu ermitteln, geht Detective wie folgt vor:
 - a. Kombiniert die prognostizierte Nutzungsdauer von 30 Tagen in allen Verhaltensdiagrammen.
 - b. Verwendet das Preismodell, um die voraussichtlichen Kosten für 30 Tage für die gesamte geplante Nutzung von 30 Tagen zu berechnen.
 4. Wenn Sie eine gemeinsam genutzte Amazon VPC verwenden, berechnet Detective die voraussichtlichen Kosten auf der Grundlage der Überwachungsaktivitäten. Wir empfehlen, dass Sie die voraussichtlichen Kosten für Ihre Untersuchungen in Ihrer jeweiligen Umgebung überprüfen.
 - a. Wenn ein Detective-Mitgliedskonto über eine gemeinsam genutzte Amazon VPC verfügt und es andere Nicht-Detective-Konten gibt, die die gemeinsam genutzte VPC verwenden, überwacht Detective den gesamten Datenverkehr von dieser VPC. Die Nutzung und die Kosten werden zunehmen und Detective bietet einen Überblick über den gesamten Datenverkehr innerhalb der VPC.
 - b. Wenn Sie eine EC2-Instance in einer gemeinsam genutzten Amazon VPC haben und der gemeinsame Eigentümer kein Detective-Mitglied ist, überwacht Detective den Datenverkehr von der VPC nicht, wodurch die Nutzung und die Kosten sinken. Wenn Sie den Datenverkehr innerhalb der VPC anzeigen möchten, müssen Sie den Eigentümer der Amazon VPC als Mitglied Ihres Detective-Diagramms hinzufügen.

Protokollieren von Amazon Detective API-Aufrufen mit AWS CloudTrail

Detective ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in Detective ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für Detective als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Detective-Konsole und Code-Aufrufe der Detective-API-Operationen.

- Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Detective.
- Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen.

Anhand der von CloudTrail gesammelten Informationen können Sie Folgendes ermitteln:

- Die Anforderung, die an Detective gestellt wurde
- Die IP-Adresse, von der die Anforderung erfolgt ist
- Wer die Anforderung gestellt hat
- Wann sie gestellt wurde.
- Zusätzliche Details zur Anforderung

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

Detektivinformationen in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn in Detective eine Aktivität auftritt, wird diese Aktivität zusammen mit anderen AWS Dienstereignissen in einem CloudTrail Ereignis im Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS -Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter [Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen](#).

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für Detective, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket.

Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können auch andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren.

Weitere Informationen finden Sie hier:

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail Unterstützte Dienste und Integrationen](#)
- [Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#)

CloudTrail protokolliert alle Detective-Operationen, die in der [Detective API-Referenz](#) dokumentiert sind.

Beispielsweise generieren Aufrufe der `DeleteMembers` Operationen `CreateMembersAcceptInvitation`, und Einträge in den CloudTrail Protokolldateien.

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
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen verbundenen Benutzer gestellt wurde
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde

Weitere Informationen finden Sie unter dem [CloudTrail UserIdentity-Element](#).

Grundlagen zu Protokolldateieinträgen in Detective

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. Zu den Ereignissen gehören Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass die Einträge nicht in einer bestimmten Reihenfolge angezeigt werden.

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

```
{
  "EventId": "f2545ee3-170f-4340-8af4-a983c669ce37",
  "Username": "JaneRoe",
  "EventTime": 1571956406.0,
  "CloudTrailEvent": "{ \"eventVersion\": \"1.05\", \"userIdentity\": { \"type\": \"AssumedRole\", \"principalId\": \"AR0AJZARKEP6WKJ5JHSUS:JaneRoe\", \"arn\": \"arn:aws:sts::111122223333:assumed-role/1A4R5SKSPGG9V/JaneRoe\", \"accountId\": \"111122223333\", \"accessKeyId\": \"AKIAIOSFODNN7EXAMPLE\", \"sessionContext\": { \"attributes\": { \"mfaAuthenticated\": \"false\", \"creationDate\": \"2019-10-24T21:54:56Z\" }, \"sessionIssuer\": { \"type\": \"Role\", \"principalId\": \"AR0AJZARKEP6WKJ5JHSUS\", \"arn\": \"arn:aws:iam::111122223333:role/1A4R5SKSPGG9V\", \"accountId\": \"111122223333\", \"userName\": \"JaneRoe\" } } }, \"eventTime\": \"2019-10-24T22:33:26Z\", \"eventSource\": \"detective.amazonaws.com\", \"eventName\": \"AcceptInvitation\", \"awsRegion\": \"us-east-2\", \"sourceIPAddress\": \"192.0.2.123\", \"userAgent\": \"aws /3 aws-sdk-java/1.11.648 Linux/4.14.133-97.112.amzn2.x86_64 OpenJDK_64-Bit_Server_VM/25.201-b09 java/1.8.0_201 vendor/Oracle_Corporation exec-env/AWS_Lambda_java8\", \"errorCode\": \"ValidationException\", \"requestParameters\": { \"masterAccount\": \"111111111111\" }, \"responseElements\": { \"message\": \"Invalid request body\" }, \"requestID\": \"8437ff99-5ec4-4b1a-8353-173be984301f\", \"eventID\": \"f2545ee3-170f-4340-8af4-a983c669ce37\", \"readOnly\": false, \"eventType\": \"AwsApiCall\", \"recipientAccountId\": \"111122223333\" }",
  "EventName": "AcceptInvitation",
  "EventSource": "detective.amazonaws.com",
  "Resources": []
},
```

Regionen und Kontingente von Amazon Detective

Beachten Sie bei der Verwendung von Amazon Detective diese Kontingente.

Detective-Regionen und -Endpunkte

Eine Liste der verfügbaren Standorte von AWS-Regionen Detective finden Sie unter [Detective Service Endpoints](#).

Kontingente von Detective

Detective hat die folgenden Kontingente, die nicht konfiguriert werden können.

Ressource	Kontingent	Kommentare
Anzahl der Mitgliedskonten	1.200	Die Anzahl der Mitgliedskonten, die ein Administratorkonto zu einem Verhalten sdiagramm hinzufügen kann.
Datenvolumen Verhalten sdiagramm – Volumenwarnung	9 TB pro Tag	Wenn das Datenvolumen des Verhalten sdiagramms mehr als 9 TB pro Tag beträgt, zeigt Detective eine Warnung an, dass sich das Verhaltensdiagramm dem maximal zulässigen Volumen nähert.
Datenvolumen im Verhalten sdiagramm – keine neuen Konten	10 TB pro Tag	Wenn das Datenvolumen des Verhalten sdiagramms größer als 10 TB pro Tag ist, können Sie dem Verhaltensdiagramm keine neuen Mitgliedskonten hinzufügen.
Datenvolumen des Verhalten sdiagramms – Stoppen der Datenaufnahme in das Verhaltensdiagramm	15 TB pro Tag	Wenn das Datenvolumen des Verhalten sdiagramms mehr als 15 TB pro Tag beträgt, beendet Detective die Aufnahme von Daten in das Verhaltensdiagramm. Die 15 TB pro Tag spiegeln sowohl das normale Datenvolumen als auch Spitzenwerte im Datenvolumen wider.

Ressource	Kontingent	Kommentare
		Um die Datenaufnahme wieder zu aktivieren, müssen Sie mit AWS Support Kontakt aufnehmen.

Internet Explorer 11 wird nicht unterstützt

Sie können Detective nicht mit Internet Explorer 11 verwenden.

Verwaltung von Tags für ein Verhaltensdiagramm

Sie können Ihrem Verhaltensdiagramm Tags zuweisen. Anschließend können Sie die Tag-Werte in IAM-Richtlinien verwenden, um den Zugriff auf Verhaltensdiagramm-Funktionen in Detective zu verwalten. Siehe [the section called “Autorisierung auf der Grundlage von Detective Behavior Diagramm-Tags”](#).

Sie können Tags auch als Tool für die Kostenberichterstattung verwenden. Um beispielsweise die mit der Sicherheit verbundenen Kosten zu verfolgen, könnten Sie Ihrem Detective-Verhaltensdiagramm, Ihrer AWS Security Hub Hub-Ressource und Ihren GuardDuty Amazon-Detektoren dasselbe Tag zuweisen. In AWS Cost Explorer könnten Sie dann nach diesem Tag suchen, um eine konsolidierte Ansicht der Kosten für diese Ressourcen zu erhalten.

Die Tags für ein Verhaltensdiagramm anzeigen (Konsole)

Sie verwalten die Tags für Ihr Verhaltensdiagramm auf der Seite Allgemein.

So zeigen Sie die Liste der Tags an, die dem Verhaltensdiagramm zugewiesen sind

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Klicken Sie im Navigationsbereich unter Settings auf General.

Auflisten der Tags für ein Verhaltensdiagramm (Detective API, AWS CLI)

Sie können die Detective API oder die verwenden AWS Command Line Interface , um die Liste der Tags für Ihr Verhaltensdiagramm abzurufen.

Um die Liste der Tags für ein Verhaltensdiagramm abzurufen (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [ListTagsForResource](#). Sie müssen den ARN Ihres Verhaltensdiagramms angeben.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl `list-tags-for-resource` aus.

```
aws detective list-tags-for-resource --resource-arn <behavior graph ARN>
```

Beispiel

```
aws detective list-tags-for-resource --resource-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Hinzufügen von Tags zu einem Verhaltensdiagramm (Konsole)

Über die Tag-Liste auf der Seite Allgemein können Sie dem Verhaltensdiagramm Tag-Werte hinzufügen.

Hinzufügen eines Tags zu Ihrem Verhaltensdiagramm

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.

Hinzufügen von Tags zu einem Verhaltensdiagramm (Detective API, AWS CLI)

Sie können die Detective API oder die verwenden AWS CLI , um Ihrem Verhaltensdiagramm Tag-Werte hinzuzufügen.

Um Tags zu einem Verhaltensdiagramm hinzuzufügen (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [TagResource](#). Sie geben den ARN des Verhaltensdiagramms und die hinzuzufügenden Tag-Werte an.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl `tag-resource` aus.

```
aws-detective tag-resource --aws detective tag-resource --resource-arn <behavior graph ARN> --tags '{"TagName":"TagValue"}
```

Beispiel

```
aws detective tag-resource --resource-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 --tags '{"Department":"Finance"}
```

Tags aus einem Verhaltensdiagramm entfernen (Konsole)

Um ein Tag aus der Liste auf der Seite Allgemein zu entfernen, wählen Sie die Option Entfernen für dieses Tag.

Tags aus einem Verhaltensdiagramm entfernen (Detective API, AWS CLI)

Sie können die Detective API oder die verwenden AWS CLI , um Tag-Werte aus Ihrem Verhaltensdiagramm zu entfernen.

Um Tags aus einem Verhaltensdiagramm zu entfernen (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [UntagResource](#). Sie geben den ARN des Verhaltensdiagramms und die Namen der zu entfernenden Tags an.
- AWS CLI: Führen Sie in der Befehlszeile den Befehl `untag-resource` aus.

```
aws detective untag-resource --resource-arn <behavior graph ARN> --tag-keys "TagName"
```

Beispiel

```
aws detective untag-resource --resource-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 --tag-keys "Department"
```

Deaktivieren von Amazon Detective

Das Administratorkonto für ein Verhaltensdiagramm kann Amazon Detective über die Detective-Konsole, die Detective-API oder AWS Command Line Interface deaktivieren. Wenn Sie Detective deaktivieren, werden das Verhaltensdiagramm und die zugehörigen Detective-Daten gelöscht.

Sobald ein Verhaltensdiagramm gelöscht wurde, kann es nicht wiederhergestellt werden.

Inhalt

- [Detective deaktivieren \(Konsole\)](#)
- [Detective deaktivieren \(Detective API, AWS CLI\)](#)
- [Detective regionsübergreifend deaktivieren \(Python-Skript aktiviert GitHub\)](#)

Detective deaktivieren (Konsole)

Sie können Amazon Detective über die AWS Management Console deaktivieren.

So deaktivieren Sie Amazon Detective (Konsole)

1. Öffnen Sie die Amazon-Detective-Konsole unter <https://console.aws.amazon.com/detective/>.
2. Klicken Sie im Detective-Navigationsbereich unter Einstellungen auf Allgemein.
3. Wählen Sie auf der Seite Allgemein unter Amazon Detective deaktivieren die Option Amazon Detective deaktivieren aus.
4. Wenn Sie dazu aufgefordert werden, geben Sie zur Bestätigung **disable** ein.
5. Wählen Sie Amazon Detective deaktivieren.

Detective deaktivieren (Detective API, AWS CLI)

Sie können Amazon Detective über die Detective API oder die AWS Command Line Interface deaktivieren. Verwenden Sie die Operation [ListGraphs](#), um den ARN Ihres Verhaltensdiagramms zur Verwendung in der Anfrage abzurufen.

Um Detective zu deaktivieren (Detective API, AWS CLI)

- Detective API: Verwenden Sie die Operation [DeleteGraph](#). Sie müssen den Diagramm-ARN angeben.

- AWS CLI: Führen Sie in der Befehlszeile den Befehl [delete-graph](#) aus.

```
aws detective delete-graph --graph-arn <graph ARN>
```

Beispiel:

```
aws detective delete-graph --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Detective regionsübergreifend deaktivieren (Python-Skript aktiviert GitHub)

Detective bietet ein Open-Source-Skript [GitHub](#) , mit dem Sie Detective für ein Administratorkonto in einer bestimmten Liste von Regionen deaktivieren können.

Informationen zur Konfiguration und Verwendung der GitHub Skripts finden Sie unter [the section called "Amazon Detective Python-Skripte"](#).

Dokumentverlauf für das Detective-Benutzerhandbuch

Die folgende Tabelle beschreibt wichtige Änderungen an der Dokumentation seit der letzten Veröffentlichung von Detective. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

- Letzte Aktualisierung der Dokumentation: 15. Mai 2024

Änderung	Beschreibung	Datum
Neue Security Lake-Quellversionen	Zusätzlich zur Quellversion 1 (OCSF 1.0.0-rc.2) nimmt Detective jetzt Daten aus Quellversion 2 (OCSF 1.1.0) für die Security Lake-Quellen auf, die von Detective unterstützt werden.	15. Mai 2024
Neue Security Lake-Protokollquelle	Sie können die Detective-Integration mit Security Lake verwenden, um Protokolle und Ereignisse aus Amazon EKS Audit Logs zu sammeln.	15. Mai 2024
Aktualisierung der Dokumentation	Der Inhalt des Amazon Detective Administration Guide ist jetzt im Amazon Detective User Guide zusammengefasst. Der Standardsupport für Amazon Detective Administration Guide endet am 08. Mai 2024.	15. April 2024
Unterstützung für GuardDuty Amazon-Ergebnisse hinzugefügt	Detective bietet jetzt Unterstützung für die folgenden Findetypen von GuardDuty Runtime Monitoring .	5. April 2024

Execution:Runtime/
MaliciousFileExecu
ted Execution
:Runtime/Suspiciou
sTool DefenseEv
asion:Runtime/
PtraceAntiDeb
ugging Execution
:Runtime/Suspiciou
sCommand DefenseEv
asion:Runtime/Susp
iciousCommand

[Die GuardDuty Amazon-Mitgliedschaftsanforderung wurde entfernt](#)

Sie müssen kein GuardDuty Kunde mehr sein, um Amazon Detective zu aktivieren. Die Anforderung, dass Detective 48 Stunden lang in Ihrem Konto GuardDuty aktiviert sein muss, bevor Detective aktiviert werden kann, wurde entfernt.

2. Februar 2024

[Unterstützung für GuardDuty Amazon-Ergebnisse hinzugefügt](#)

Detective erweitert die Unterstützung für die Suche nach Typen von [GuardDuty EC2 Runtime Monitoring](#) auf ECS- und EC2-Ressourcen.

30. Januar 2024

Aktualisierte Funktionalität

Sie können jetzt auf der Seite Ermittlungen eine Detektivuntersuchung für eine bestimmte Ressource durchführen, die Sie untersuchen möchten. Detective empfiehlt Ressourcen auf der Grundlage seiner Aktivitäten in Erkenntnissen und Erkenntnisgruppen. Mit [Detective Investigations](#) können Sie IAM-Benutzer und IAM-Rollen anhand von Bedrohungssindikatoren untersuchen, anhand derer Sie feststellen können, ob eine Ressource an einem Sicherheitsvorfall beteiligt ist.

16. Januar 2024

Aktualisierte Funktionalität

Sie können jetzt eine Detektiv-Untersuchung auf der Seite „Untersuchungen“ für eine empfohlene Ressource durchführen. Detective empfiehlt Ressourcen auf der Grundlage seiner Aktivitäten in Erkenntnissen und Erkenntnisgruppen. Mit [Detective Investigations](#) können Sie IAM-Benutzer und IAM-Rollen anhand von Bedrohungssindikatoren untersuchen, anhand derer Sie feststellen können, ob eine Ressource an einem Sicherheitsvorfall beteiligt ist.

26. Dezember 2023

[Änderungen in der Art und Weise, wie Detective den Datenverkehr für gemeinsam genutzte VPCs liest](#)

Wenn Sie eine gemeinsam genutzte Amazon VPC verwenden, stellen Sie vielleicht Änderungen im von Detective überwachten Datenverkehr fest. Wir empfehlen Ihnen, die Änderungen in den [Aktivitätsdetails für das gesamte VPC-Durchflussvolumen](#) zu überprüfen, um die möglichen Auswirkungen auf Ihre Abdeckung zu verstehen, und zu erfahren, [wie Detective die voraussichtlichen Kosten berechnet](#), um nachzuziehen, wie sich dies auf Ihre Servicekosten auswirken kann.

20. Dezember 2023

[Regionale Verfügbarkeit](#)

Die Regionen Europa (Stockholm), Europa (Paris) und Kanada (Zentral) wurden zur Liste der AWS Regionen hinzugefügt, in denen die [Detective-Integration mit Security Lake](#) verfügbar ist.

8. Dezember 2023

[Neues Feature](#)

Mit [Detective-Untersuchungen](#) können Sie IAM-Benutzer und IAM-Rollen anhand von Bedrohungsindikatoren untersuchen, anhand derer Sie feststellen können, ob eine Ressource an einem Sicherheitsvorfall beteiligt ist.

26. November 2023

Neues Feature

Standardmäßig generiert Detective automatisch [Erkenntnisgruppenübersichten](#) für Erkenntnisgruppen, die auf generativer künstlicher Intelligenz (generativer KI) basieren. Die Erkenntnisgruppenübersicht analysiert schnell die Beziehungen zwischen den Erkenntnissen und den betroffenen Ressourcen und fasst anschließend potenzielle Bedrohungen in natürlicher Sprache zusammen.

26. November 2023

Neues Feature

[Mit der Integration von Detective mit Security Lake](#) können Sie die von Security Lake gespeicherten Rohprotokolldaten abfragen und abrufen. Mithilfe dieser Integration können Sie Protokolle und Ereignisse von CloudTrail Verwaltungsereignissen und Amazon Virtual Private Cloud (Amazon VPC) Flow Logs sammeln.

26. November 2023

Informationen zu verwalteten Richtlinien zum Kapitel Sicherheit hinzugefügt

Der AmazonDetectiveInvestigatorAccess - Richtlinie wurden die Aktionen Detective-Untersuchungen und Erkenntnisgruppen hinzugefügt.

26. November 2023

Erkenntnisübersicht anzeigen	Wenn eine Erkenntnis mit einer größeren Aktivität korreliert, fordert Detective Sie jetzt auf, zu dieser Erkenntnisgruppe zu navigieren.	18. September 2023
Endpunkte und Kontingente von Amazon Detective	Detective ist jetzt in der Region Israel (Tel Aviv) verfügbar.	25. August 2023
Verbesserte Visualisierung von Erkenntnisgruppen	Visualisierung von Erkenntnisgruppen in Detective umfasst jetzt auch Erkenntnisgruppen mit aggregierten Erkenntnissen, was die Analyse verwandter Beweise, Entitäten und Erkenntnisse effizienter gestaltet.	08. August 2023
Erweiterterte Erkenntnisgruppen	Zu den Erkenntnisgruppen gehören jetzt auch Sicherheitslücken von Amazon Inspector.	13. Juni 2023
Unterstützung für Amazon GuardDuty Lambda Protection hinzugefügt	Detective bietet jetzt Unterstützung für GuardDuty Lambda Protection.	26. Mai 2023
AWS Sicherheitsergebnisse wurden als neues optionales Datenquellenpaket hinzugefügt.	Detective stellt jetzt AWS Sicherheitsergebnisse als optionales Datenquellenpaket bereit. Mit diesem optionalen Datenquellenpaket kann Detective Daten aus Security Hub aufnehmen und diese Daten Ihrem Verhaltensdiagramm hinzufügen.	16. Mai 2023

Unterstützung für Suchtypen von Amazon GuardDuty EKS Runtime Monitoring hinzugefügt	Detective bietet jetzt Unterstützung für die GuardDuty Suchtypen von EKS Runtime Monitoring.	3. Mai 2023
Unterstützung für Suchtypen von Amazon GuardDuty RDS Protection hinzugefügt	Detective unterstützt jetzt Suchtypen für den GuardDuty RDS-Schutz.	20. April 2023
Unterstützung für weitere GuardDuty Amazon-Suchtypen hinzugefügt	Detective bietet jetzt Profile für die folgenden zusätzlichen GuardDuty Findetypen: DefenseEvasion: EC2UnusualDNSResolver DefenseEvasion: EvasionEC2UnusualDoHActivity DefenseEvasion: DefenseEvasionEC2UnusualDoTActivity	12. April 2023
In der Detective-Konsole wurden neue Konsolenbereiche hinzugefügt, um Benutzern bei der Auswahl einer geeigneten von AWS verwalteten Richtlinie für ihren spezifischen Anwendungsfall zu helfen.	Detective bietet verwaltete Richtlinien für eine sichere Auswahl von Berechtigungen, die Sie benötigen.	03. April 2023
Anzeige des VPC-Datendurchflussverkehrs für EKS-Cluster	Neuer Abschnitt für Amazon Virtual Private Cloud (Amazon VPC)-Datendurchflussverkehr mit Amazon Elastic Kubernetes Service (Amazon EKS)-Clustern hinzugefügt.	2. März 2023

[Erkenntnisgruppe beinhaltet jetzt eine dynamische visuelle Darstellung des Verhaltensdiagramms von Detective](#)

Die Detective-Erkenntnisgruppe enthält jetzt eine dynamische visuelle Darstellung des Verhaltensdiagramms von Detective, um die Beziehung zwischen Entitäten und Erkenntnissen innerhalb der Erkenntnisgruppe hervorzuheben.

28. Februar 2023

[Exportieren Sie Daten von der Seite Übersicht in Detective und der Suchergebnisseite. Die Daten werden im CSV-Format \(komma-getrennte Werte\) exportiert.](#)

Detective bietet jetzt die Möglichkeit, Daten aus der Detective-Konsole in Ihren Browser zu exportieren.

07. Februar 2023

[Gesamt-VPC-Datendurchfluss-Volumen für EKS Amazon-EKS-Workloads hinzugefügt](#)

Detective fügt jetzt visuelle Übersichten und Analysen zu Ihren Amazon Virtual Private Cloud (VPC)-Datendurchfluss-Protokollen aus Ihren Amazon Elastic Kubernetes Service Amazon EKS-Workloads hinzu.

19. Januar 2023

[Informationen zu verwalteten Richtlinien zum Kapitel Sicherheit hinzugefügt](#)

Detective unterstützt GuardDuty jetzt im Rahmen der AmazonDetectiveFullAccess Richtlinie Maßnahmen zum Abrufen von Erkenntnissen. Das Sicherheitskapitel enthält jetzt Einzelheiten zu den folgenden neuen verwalteten Richtlinien für Detective : AmazonDetectiveMemberAccess und AmazonDetectiveInvestigatorAccess.

17. Januar 2023

[Datenaufbewahrung hinzugefügt](#)

Mit Detective können Sie auf historische Ereignisdaten von bis zu einem Jahr zugreifen.

20. Dezember 2022

[Auf der Übersichtsseite wurde die Option zur Anpassung der Gültigkeitsdauer hinzugefügt.](#)

Detective bietet jetzt die Möglichkeit, den Zeitrahmen so anzupassen, dass Sie sich die Aktivität für einen beliebigen 24-Stunden-Zeitraum der letzten 365 Tage ansehen können.

5. Oktober 2022

[Suche nach einer Erkenntnis oder Entität](#)

Detective bietet jetzt eine Suche ohne Berücksichtigung von Groß- und Kleinschreibung.

3. Oktober 2022

[Möglichkeit zum Setzen des Zeitstempels für den Geltungsbereich hinzugefügt](#)

Detective bietet jetzt eine Möglichkeit, die Einstellung für das Format des Bereichszeitstempels zu konfigurieren. Diese Einstellung wird auf alle Zeitstempel in Detective angewendet.

3. Oktober 2022

[Es wurden Begriffe hinzugefügt, die sich auf Erkenntnisgruppen beziehen](#)

Detective unterstützt jetzt Suchgruppen, die verwandte Erkenntnisse auf einer einzigen Anzeige miteinander verbinden, um Sie bei der Untersuchung potenzieller bössartiger Aktivitäten in Ihrer Umgebung zu unterstützen. Von einem Suchgruppenprofil aus können Sie zu Entitätsprofilen wechseln und nach Übersichten suchen, die sich auf diese Gruppe beziehen.

03. August 2022

[Es wurden neue Profile hinzugefügt, die mit Amazon-EKS-Auditprotokollen verknüpft sind](#)

Detective stellt jetzt Profile bereit, mit denen Sie Aktivitäten im Zusammenhang mit den folgenden containerbezogenen Entitäten untersuchen können: Amazon-EKS-Cluster, Container-Images, Kubernetes-Pods und Kubernetes-Themen.

26. Juli 2022

[Neue optionale Datenquelle hinzugefügt](#)

Detective unterstützt jetzt EKS-Auditprotokolle als optionales Datenquellenpaket. Ein Administratorkonto kann diese neue Datenquelle für sein vorhandenes Verhalten sdiagramm aktivieren. Bei Diagrammen, die nach diesem Datum erstellt wurden, ist diese Datenquelle standardmäßig aktiviert. Administratoren können diese Datenquelle jederzeit manuell deaktivieren.

26. Juli 2022

[Neue serviceverknüpfte Rolle und verwaltete Richtlinie für Detective](#)

Detective hat jetzt eine dienstbezogene Rolle, `AWSServiceRoleForDetective`. Die serviceverknüpfte Rolle wird verwendet, um in Ihrem Namen auf Organisations-Daten zuzugreifen. Die Rolle verwendet eine neue `AmazonDetectiveServiceLinkdRolePolicy`-verwaltete Richtlinie.

16. Dezember 2021

[Integration mit hinzugefügt
AWS Organizations](#)

Detective ist jetzt in Organisations integriert. Das Organisationsverwaltungs-konto weist ein Detective-Administrator-konto für die Organisation aus. Das Detective-Administrator-konto kann alle Konten in der Organisation anzeigen und diese Konten als Mitglieds-konten im Diagramm zum Organisationsverhalten aktivieren.

16. Dezember 2021

[Erkenntnisprofile wurden
durch Erkenntnisübersichten
ersetzt](#)

Die Suche nach Profilen enthielt Visualisierungen, in denen die Aktivitäten der betreffenden Ressource analysiert wurden. Die neue Ergebnisübersicht enthält Informationen zu den Ergebnissen, die von den beteiligten Entitäten aufgenommen GuardDuty wurden, und eine Liste der beteiligten Entitäten. Von der Erkenntnisübersicht aus können Sie zu den Profilen verwandter Entitäten wechseln.

20. September 2021

[Die Beschränkung der unterstützten GuardDuty Findertypen wurde aufgehoben](#)

Detective ist nicht mehr auf einen ausgewählten Satz von GuardDuty Findertypen beschränkt. Detective sammelt automatisch Funddetails für alle Erkenntnistypen und bietet Zugriff auf die Entitätsprofile für die zugehörigen Entitäten.

20. September 2021

[Link zu den Erkenntnisdetails im zugehörigen Erkenntnisprofilbereich](#)

Wenn Sie in einem Entitätsprofil eine Erkenntnis in der zugehörigen Erkenntnisliste auswählen, werden die Erkenntnisdetails im Bereich auf der rechten Seite angezeigt. Die Gültigkeitsdauer ist auf das Zeitfenster für die Suche festgelegt.

20. September 2021

[S3-Buckets zu den verfügbaren Entitätstypen in Detective hinzugefügt](#)

Detective stellt jetzt Profile für S3-Buckets bereit. Die S3-Bucket-Profilen enthalten Details zu den Prinzipalen, die mit dem S3-Bucket interagiert haben, und zu den API-Vorgängen, die sie auf dem S3-Bucket ausgeführt haben.

20. September 2021

[Neue Option zum Generieren von Detective-URLs in Splunk](#)

Das Splunk Trumpet-Projekt ermöglicht es Ihnen, AWS Inhalte an Splunk zu senden. Das Projekt ermöglicht es Ihnen jetzt, Detektiv-URLs hinzuzufügen, um zu Profilen für GuardDuty Ergebnisse zu navigieren.

8. September 2021

[AKIDs wurden in den Aktivitätsdetails für Konten und Rollen ersetzt](#)

In Kontoprofilen werden in den Aktivitätsdetails für das Gesamte API-Aufrufvolumen jetzt Benutzer oder Rollen anstelle von Zugriffsschlüsselennungen (AKIDs) angezeigt . In Rollenprofilen werden in den Aktivitätsdetails für das Gesamte API-Aufrufvolumen jetzt Rollensitzungen statt AKIDs angezeigt. Bei Aktivitäten, die vor dieser Änderung stattfanden, wird der Aufrufer als Unbekannte Ressource aufgeführt.

14. Juli 2021

[Der Aufrufdienst wurde zu den Informationen über API-Aufrufe hinzugefügt](#)

In der Detective-Konsole enthalten die Informationen zu API-Aufrufen jetzt den Dienst, der den Aufruf ausgelöst hat. Zu den Listen mit dem Gesamtvolumen der API-Aufrufe, den Neu beobachteten API-Aufrufen und den API-Aufrufen mit erhöhtem Volumen wurde eine Spalte Dienst hinzugefügt. In den Aktivitätsdetails für Gesamtes API-Aufrufvolumen und Neu beobachtete Geolocations sind die API-Methoden nach den Diensten gruppiert, die sie ausgegeben haben. Für Aktivitäten, die vor dieser Änderung stattfanden, werden die API-Methoden unter Unbekannter Dienst gruppiert.

14. Juli 2021

[Neue Registerkarte Ressourcenerweiterung für Benutzer, Rollen und Rollensitzungen](#)

Die Registerkarte Interaktion mit Ressourcen für Benutzer, Rollen und Rollensitzungen enthält Informationen über Aktivitäten zur Übernahme von Rollen, an denen diese Entitäten beteiligt waren. Für Rollensitzungen ist dies eine neue Registerkarte. Für Benutzer und Rollen ist dies eine bestehende Registerkarte mit neuen Inhalten.

29. Juni 2021

[Werte für Verhaltensdiagramme, Datenvolumenkontingente aktualisiert.](#)

Die Datenvolumenquoten für Verhaltensdiagramme wurden erhöht. Bei 3,24 TB pro Tag gibt Detective eine Warnung aus. Bei 3,6 TB pro Tag können keine neuen Konten hinzugefügt werden. Bei 4,5 TB pro Tag hört Detective auf, Daten in das Verhaltensdiagramm aufzunehmen.

10. Juni 2021

[Tag-Werte zu den Python-Skriptoptionen hinzugefügt](#)

Wenn Sie das Detective-Python-Skript `enableDetective.py` verwenden, um Detective zu aktivieren, können Sie dem Verhaltensdiagramm jetzt Tag-Werte zuweisen.

19. Mai 2021

[Automatische Aktivierung von Mitgliedskonten hinzugefügt, die die Datenvolumenprüfung bestehen](#)

Wenn Mitgliedskonten eine Einladung annehmen, lautet ihr Status Akzeptiert (Nicht aktiviert), bis Detective sichergestellt hat, dass ihre Daten nicht dazu führen, dass das Datenvolumen des Verhaltensdiagramms das Kontingent überschreitet. Wenn das Datenvolumen kein Problem darstellt, ändert Detective den Status automatisch auf Akzeptiert (Aktiviert). Beachten Sie, dass bestehende Mitgliedskonten, die derzeit Akzeptiert (nicht aktiviert) sind, nicht automatisch aktiviert werden können.

12. Mai 2021

[Informationen zu verwalteten Richtlinien zum Kapitel Sicherheit hinzugefügt](#)

Ein neuer Abschnitt im Kapitel Sicherheit enthält Einzelheiten zu verwalteten Richtlinien für Detective. Detective bietet derzeit eine einzige verwaltete Richtlinie, `AmazonDetectiveFullAccess`.

10. Mai 2021

[Datenvolumenwerte in der Liste der Mitgliedskonten geändert](#)

Auf der Kontoverwaltungsseite zeigt die Liste der Mitgliedskonten jetzt das tägliche Datenvolumen für jedes Mitgliedskonto an. Bisher wurde in der Liste das Volumen als Prozentsatz des gesamten zulässigen Volumens angezeigt.

29. April 2021

[Optionen für die Verwaltung von Mitgliedskonten überarbeitet](#)

Das Menü Konten verwalten wurde durch ein Aktionsmenü ersetzt. Kombiniert die Optionen zum Hinzufügen einzelner Konten und zum Hinzufügen von Konten aus einer CSV-Datei. Konten aktivieren wurde von Konten verwalten in eine separate Option neben Aktionen verschoben.

05. April 2021

[Tags für Verhaltensdiagramme und Autorisierung auf der Basis von Tags hinzugefügt](#)

Wenn Sie Detective aktivieren, können Sie dem Verhaltensdiagramm Tags hinzufügen. Sie können Tags für Verhaltensdiagramme auf der Seite Allgemein verwalten. Detective unterstützt auch die Autorisierung auf der Grundlage von Tag-Werten.

31. März 2021

[Unterstützung für weitere GuardDuty Amazon-Suchtypen hinzugefügt](#)

Detective bietet jetzt Profile für die folgenden zusätzlichen GuardDuty Findertypen: CredentialAccess:IAMUser/AnomalousBehavior, DefenseEvasion:IAMUser/AnomalousBehavior, Discovery:IAMUser/AnomalousBehavior, Exfiltration:IAMUser/AnomalousBehavior, Impact:IAMUser/AnomalousBehavior, InitialAccess:IAMUser/AnomalousBehavior, Persistence:IAMUser/AnomalousBehavior, PrivilegeEscalation:IAMUser/AnomalousBehavior

29. März 2021

[Es wurden Unterschiede für AWS GovCloud \(US\) Regionen hinzugefügt](#)

Detective ist jetzt in den AWS GovCloud (US) Regionen verfügbar. In AWS GovCloud (US-Ost) und AWS GovCloud (US-West) sendet Detective keine Einladungs-E-Mails an Mitgliedskonten. Detective entfernt auch nicht automatisch Mitgliedskonten, die in AWS geschlossen wurden.

24. März 2021

[Tabs hinzugefügt, um die Liste der Mitgliedskonten nach dem Status des Mitgliedskontos zu filtern](#)

In der Liste der Mitgliedskonten werden jetzt Tabs angezeigt, mit denen Sie die Liste nach dem Status des Mitgliedskontos filtern können. Sie können alle Mitgliedskonten anzeigen, sowohl solche mit dem Status Akzeptiert (Aktiviert) als auch solche, die einen anderen Status als Akzeptiert (Aktiviert) haben.

16. März 2021

[Unterstützung für weitere GuardDuty Amazon-Suchtypen hinzugefügt](#)

Detective bietet jetzt Profile für die folgenden zusätzlichen GuardDuty Findetypen: Backdoor:EC2/C&CActivity.B Impact:EC2/PortSweep , Impact:EC2/WinRMBruteForce , und PrivilegeEscalation:IAMUser/AdministrativePermissions

4. März 2021

[Option zum Python-Skript hinzugefügt, um Einladungs-E-Mails zu unterdrücken](#)

Das Detective enableDetective.py -Skript bietet jetzt eine --disable_email -Option. Wenn Sie diese Option angeben, sendet Detective keine Einladungs-E-Mails an die Mitgliedskonten.

26. Februar 2021

[„Hauptkonto“ wurde in „Administratorkonto“ geändert.](#)

Der Begriff „Hauptkonto“ wird in „Administratorkonto“ geändert. Der Begriff wurde auch in der Detective-Konsole und der API geändert.

25. Februar 2021

[„Hauptkonto“ wurde in „Administratorkonto“ geändert.](#)

Der Begriff „Hauptkonto“ wird in „Administratorkonto“ geändert. Der Begriff wurde auch in der Detective-Konsole und der API geändert.

25. Februar 2021

[Aktivitätsdetails für das VPC-Datendurchfluss-Volumen im Profilbereich zur und von der IP-Adresse der Erkenntnis hinzugefügt](#)

Das VPC-Datendurchfluss-Volumen zur und von der IP-Adresse des Erkenntnisses im Profilbereich ermöglicht es Ihnen jetzt, Aktivitätsdetails anzuzeigen. Die Aktivitätsdetails sind nur verfügbar , wenn die Erkenntnis mit einer einzigen IP-Adresse verknüpft ist. Die Aktivitätsdetails zeigen das Volumen für jede Kombination von Ports, Protokoll und Richtung.

25. Februar 2021

[API-Option hinzugefügt, um keine Einladungs-E-Mails an Mitgliedskonten zu senden](#)

Wenn Administratorkonten mithilfe der Detective API Mitgliedskonten hinzugefügt werden, können sie festlegen, dass keine Einladungs-E-Mails an Mitgliedskonten gesendet werden.

25. Februar 2021

[Neue Aktivitätsdetails für den Profildbereich „Gesamtes API-Aufrufvolumen“ in IP-Adressprofilen](#)

Sie können jetzt Aktivitätsdetails für IP-Adressen im Profildbereich für das Allgemeine API-Aufrufvolumen anzeigen. Die Aktivitätsdetails zeigen die Anzahl der erfolgreichen und fehlgeschlagenen Aufrufe für jede Ressource, die den Aufruf von der IP-Adresse aus getätigt hat.

23. Februar 2021

[Neues Fenster für den allgemeinen Profildbereich für das VPC-Datendurchflussvolumen in IP-Adressprofilen](#)

Das IP-Adressprofil enthält jetzt den Profildbereich Gesamt-VPC-Datendurchflussvolumen. Im Profildbereich wird das Volumen des VPC-Datenverkehrs zur und von der IP-Adresse angezeigt. Sie können Aktivitätsdetails anzeigen, um das Volumen für jede EC2-Instance anzuzeigen, mit der die IP-Adresse kommuniziert hat.

21. Januar 2021

[Seite Detective-Übersicht hinzugefügt](#)

Die Seite Detective Übersicht enthält Visualisierungen, die Analysten anhand von Geolocation, Anzahl der API-Aufrufe und Amazon-EC2-Datenverkehrsvolumen zu interessanten Entitäten führen.

21. Januar 2021

[Die Option, von Amazon GuardDutyIn zu Detective GuardDuty zu wechseln, wurde aktualisiert](#)

GuardDutyIn wurde die Option In Detective untersuchen vom Menü Aktionen in den Bereich mit den Ergebnisdetails verschoben. Sie zeigt eine Liste verwandter Entitäten an. Wenn der Erkenntnistyp unterstützt wird, enthält die Liste auch die Erkenntnis. Sie können dann wählen, ob Sie zu einem Entitätsprofil oder einem Suchprofil navigieren möchten.

15. Januar 2021

[Option hinzugefügt, um das Fenster mit den Aktivitätsdetails auf die Standardbereichszeit einzustellen](#)

In den Aktivitätsdetails für das Gesamte API-Aufrufvolumen und das Gesamte VPC-Datendurchfluss-Volumen können Sie das Zeitfenster für die Aktivitätsdetails auf die Standardumfangszeit für das Profil festlegen.

15. Januar 2021

[Handhabung von Zeitintervallen mit hohem Volumen für Entitäten hinzugefügt](#)

Es wurde ein neuer Hinweis hinzugefügt, der angibt, wann eine Entität über ein oder mehrere Zeitintervalle mit hohem Volumen verfügt. Auf einer neuen Seite mit Entitäten mit hohem Volumen werden alle Intervalle mit hohem Volumen für den aktuellen Gültigkeitszeitraum angezeigt.

18. Dezember 2020

[Kontingent für Mitgliedskonten auf 1.200 erhöht](#)

Hauptkonten können jetzt bis zu 1.200 Mitgliedskonten zu ihrem Verhaltensdiagramm einladen. Zuvor war die Quote 1.000.

11. Dezember 2020

[Werte für Datenvolumenkontingente in Verhaltensdiagrammen hinzugefügt](#)

Die Informationen über Datenvolumenkontingente in Verhaltensdiagrammen wurden aktualisiert, um die spezifischen Kontingentwerte hinzuzufügen.

11. Dezember 2020

[Zeitbereichsauswahl für Aktivitätsdetails im Profilbereich für das Gesamt-API-Aufrufvolumen hinzugefügt](#)

Im Bereich Gesamtes API-Datendurchflussvolumen können Sie jetzt Aktivitätsdetails für jeden ausgewählten Zeitraum anzeigen. Im Bereich wird zunächst eine Option zur Anzeige der Aktivitätsdetails für den Zeitbereich angezeigt.

29. September 2020

[Zeitintervallauswahl für Aktivitätsdetails im Profilbereich „Gesamtes VPC-Datendurchfluss-Volumen“ hinzugefügt](#)

Im Bereich Gesamtes VPC-Datendurchfluss-Volumen können Sie Aktivitätsdetails für ein einzelnes Zeitintervall aus dem Diagramm anzeigen. Um die Details für das Zeitintervall anzuzeigen, wählen Sie das Zeitintervall aus.

25. September 2020

[Neue Rollensitzung und verbundene Benutzerentitäten](#)

Detective ermöglicht es Ihnen jetzt, die Verbundauthentifizierung zu prüfen und zu untersuchen. Sie können sehen, welche Ressourcen die einzelnen Rollen übernommen haben und wann diese Authentifizierungen stattgefunden haben.

17. September 2020

[Aktualisierungen der Zeitbereichsverwaltung](#)

Die Option zum Sperren oder Entsperrern des Zeitbereichs wurde entfernt. Sie ist immer gesperrt. In einem Erkenntnisprofil wird eine Warnung angezeigt, wenn die Gültigkeitsdauer des Suchbereichs vom Zeitfenster für die Suche abweicht.

4. September 2020

[Die Profilkopfzeile bleibt sichtbar, wenn Sie durch ein Profil blättern](#)

Bei Profilen bleiben Typ, ID und Zeitbereich sichtbar, wenn Sie auf einer Registerkarte durch die Profilbereiche blättern. Wenn die Tabs nicht sichtbar sind, können Sie die Registerkarten-Dropdown-Liste in den Breadcrumbs verwenden, um zu einer anderen Registerkarte zu wechseln.

4. September 2020

[Bei der Suche werden immer Suchergebnisse angezeigt](#)

Wenn Sie eine Suche durchführen, werden die Ergebnisse jetzt auf der Erkenntniseite angezeigt . Von den Erkenntnissen aus können Sie zu einem Erkenntnis- oder Entitätsprofil wechseln.

27. August 2020

[Zulässige Suchkriterien ergänzt](#)

Die zulässigen Kriterien für Suchanfragen wurden erweitert. Sie können anhand des Namens nach AWS Benutzern und AWS Rollen suchen. Sie können den ARN verwenden, um nach Ergebnissen, AWS Rollen, AWS Benutzern und EC2-Instances zu suchen.

27. August 2020

[Links zu anderen Konsolen in den Profilbereichen](#)

Im Profilbereich mit den EC2-Instance-Details ist die EC2-Instance-ID mit der Amazon-EC2-Konsole verknüpft. In den Profilbereichen Benutzerdetails und Rollendetails sind der Benutzername und der Rollenname mit der IAM-Konsole verknüpft.

14. August 2020

[Aktivitätsdetails für VPC-Daten durchfluss-Daten](#)

Der Profilbereich Gesamtes VPC-Datendurchfluss-Volumen bietet jetzt Zugriff auf Aktivitätsdetails. Die Aktivitätsdetails zeigen den Datenverkehr zwischen IP-Adressen und einer EC2-Instance während eines ausgewählten Zeitraums.

23. Juli 2020

[Mitgliedskonten können jetzt ihre Nutzung und die voraussichtlichen Kosten einsehen](#)

Mitgliedskonten können jetzt ihre eigenen Nutzungsinformationen einsehen. Bei Mitgliedskonten wird auf der Seite Nutzung die Datenmenge angezeigt, die in jedes Verhaltensdiagramm aufgenommen wurde, zu dem sie beiträgt. Mitgliedskonten können auch ihre voraussichtlichen 30-Tage-Kosten sehen.

26. Mai 2020

[Die kostenlose Testversion ist jetzt pro Konto statt pro Verhaltensdiagramm verfügbar](#)

Jedes Amazon-Detective-Konto erhält jetzt in jeder Region eine separate kostenlose Testversion. Die kostenlose Testversion beginnt entweder, wenn das Konto Detective aktiviert, oder wenn das Konto zum ersten Mal als Mitgliedskonto aktiviert wird.

26. Mai 2020

[Neue Open-Source-Python-Skripte auf GitHub](#)

Das neue [amazon-detective-multiaccount-scripts](#) Repository on GitHub bietet Open-Source-Python-Skripte, mit denen Sie Verhalten sdiagramme in verschiedenen Regionen verwalten können. Sie können Detective aktivieren, Mitgliedskonten hinzufügen, Mitgliedskonten entfernen und Detective deaktivieren.

21. Januar 2020

[Wir stellen vor: Amazon Detective](#)

Detective verwendet Machine Learning und speziell entwickelte Visualisierungen, um Sie bei der Analyse und Untersuchung von Sicherheitsproblemen in Ihren Amazon Web Services (AWS)-Workloads zu unterstützen.

02. Dezember 2019

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.